CONTRACT NAS9-9953 MSC 02478
DRL NO: MSC T-575, LINE ITEM 75

SD 71-224

MODULAR space station

PHASE B EXTENSION

SAFETY ANALYSIS REPORT

PREPARED BY PROGRAM ENGINEERING
30 NOVEMBER 1971

Space Division
North American Rockwell

12214 Lakewood Boulevard, Downey, California 90241

CONTRACT NAS9-9953 MSC 02478
DRL NO: MSC T-575, LINE ITEM 75

SD 71-224

MODULAR
space station
PHASE B EXTENSION

SAFETY ANALYSIS REPORT

30 NOVEMBER 1971

PREPARED BY PROGRAM ENGINEERING

Approved by

Earl G. Cole

E.G. Cole
Program Manager
Space Station Program

Space Division
North American Rockwell

12214 Lakewood Boulevard, Downey, California 90241

TECHNICAL REPORT INDEX/ABSTRACT

ACCESSION NUMBER						DOCUMENT SECURITY CLASSIFICATION	
						UNCLASSIFIED	

TITLE OF DOCUMENT
MODULAR SPACE STATION SAFETY ANALYSIS REPORT

LIBRARY USE ONLY

AUTHOR(S)

CODE	ORIGINATING AGENCY AND OTHER SOURCES	DOCUMENT NUMBER
QN085057	NORTH AMERICAN ROCKWELL CORPORATION SPACE DIVISION, DOWNEY, CALIFORNIA	SD 71-224

PUBLICATION DATE	CONTRACT NUMBER
30 NOV 1971	NAS9-9953

DESCRIPTIVE TERMS
MODULAR SPACE STATION - SAFETY ANALYSIS REPORT - HAZARD ANALYSIS - SAFETY CRITERIA - TRADE STUDIES

ABSTRACT

THIS VOLUME DOCUMENTS THE SYSTEM SAFETY ANALYSES AND REQUIREMENTS DEVELOPED FOR THE MODULAR SPACE STATION DURING THE PHASE B EXTENSION PERIOD STUDY. RESIDUAL HAZARDS AND UNRESOLVED SAFETY ISSUES ARE SUMMARIZED IN SECTION 1.

HAZARDS RESULTING FROM EQUIPMENT FAILURES OR MALFUNCTIONS, OPERATIONS OR CREDIBLE ACCIDENTS ARE IDENTIFIED AND EVALUATED. SAFETY CRITERIA AND DESIGN REQUIREMENTS ARE DOCUMENTED. SPECIAL SAFETY TRADE STUDIES ARE PRESENTED.

FOREWORD

This document is one of a series required by Contract NAS9-9953, Exhibit C, Statement of Work for Phase B Extension-Modular Space Station Program Definition. It has been prepared by the Space Division, North American Rockwell Corporation, and is submitted to the National Aeronautics and Space Administration's Manned Spacecraft Center, Houston, Texas, in accordance with the requirements of Data Requirements List (DRL) MSC-T-575, Line Item 75.

Total documentation products of the extension period are listed in the following chart in categories that indicate their purpose and relationship to the program.

ADMINISTRATIVE REPORTS	TECHNICAL REPORTS		STUDY PROGRAMMATIC REPORTS	DOCUMENTATION FOR PHASES C AND D	
				SPECIFICATIONS	PLANNING DATA
EXTENSION PERIOD STUDY PLAN DRL-62 DRD MA-207T SD 71-201	MSS PRELIMINARY SYSTEM DESIGN DRL-68 DRD SE-371T SD 71-217	MSS DRAWINGS DRL-67 DRD SE-370T SD 71-216	EXTENSION PERIOD EXECUTIVE SUMMARY DRL-65 DRD MA-012 SD 71-214	MSS PRELIMINARY PERFORMANCE SPECIFICATIONS DRL-66 DRD SE-369T SD 71-215	MSS PROGRAM MASTER PLAN DRL-76 DRD MA-209T SD 71-225
QUARTERLY PROGRESS REPORTS DRL-64 DRD MA-208T SD 71-213, -235, -576	MSS MASS PROPERTIES DRL-69 DRD SE-372T SD 71-218, -219	MSS MOCKUP REVIEW AND EVALUATION DRL-70 DRD SE-373T SD 71-220			MSS PROGRAM COST AND SCHEDULE ESTIMATES DRL-77 DRD MA-013(REV. A) SD 71-226
FINANCIAL MANAGEMENT REPORTS DRL-63 DRD MF-004	MSS INTEGRATED GROUND OPERATIONS DRL-73 DRD SE-376T SD 71-222	MSS KSC LAUNCH SITE SUPPORT DEFINITION DRL-61 DRD AL-005T SD 71-211			MSS PROGRAM OPERATIONS PLAN DRL-74 DRD SE-377T SD 71-223
	MSS SHUTTLE INTERFACE REQUIREMENTS DRL-71 DRD SE-374T SD 71-221	INFORMATION MANAGEMENT ADVANCED DEVELOPMENT DRL-72 DRD SE-375T SD 72-11			
	MSS SAFETY ANALYSIS DRL-75 DRD SA-032T SD 71-224				

CONTENTS

ILLUSTRATIONS

TABLES

1.0 INTRODUCTION AND SUMMARY

This report documents the system safety analyses and requirements developed during the Modular Space Station definition study, and fulfills the contractual requirement for a Safety Analysis Report (DRL 75). Safety criteria are based on and consistent with those used in the earlier Saturn V launched station definition studies. Hazards related to design and operations are identified and residual hazards and unresolved safety issues are documented herein. Safety criteria are also documented in the Preliminary Performance Specification (DRL 66) Section 3.1, Performance Requirements. Safety design requirements are integrated with the Subsystem Design Requirements in Section 3.3 of DRL 66.

1.1 GOALS

Since an objective of the Space Station Program is to develop routine space operations, a very high degree of system safety must be achieved. This was emphasized in the Modular Space Station definition study by defining a program-level system safety goal in the Guidelines and Constraints as follows:

> Safety is a mandatory consideration through the total program. As a goal, no single malfunction or credible combination of malfunctions and/or accidents shall result in serious injury to personnel or to crew abandonment of the space station.

As safety criteria and design and operational requirements were developed for the MSS program, they were tested against this goal to achieve consistency. Other sources for safety requirements included the Guidelines and Constraints and prior Space Station programs as applicable.

1.2 SAFETY ANALYSIS

Following the initial definition of safety criteria the system safety effort concentrated on evaluation of design and operational concepts considered in the concept trade studies. This process involved identification of potential hazards, determination of the effects of the hazards and identifying means for eliminating or reducing the hazards.

During the preliminary design of the final integrated concept the hazard analysis was conducted in depth as follows:

Identification of Potential Hazards

Hazardous equipment, hazardous operations and potential hazards inherent in the selected preliminary design and operations were identified by system safety and subsystem design personnel working on the program. A potential

hazard was one which could occur, regardless of how unlikely or improbable its occurrence may have been, and could be identified from the following sources:

- o Hazardous equipment
- o Hazardous operations
- o Normal operations
- o Credible accidents
- o Hardware failures with hazardous effects from the Critical Function Analyses

These were identified by subsystem and assembly, and by mission phase (for hazardous operations).

Determination of Effects of Hazards

The potential effect(s) of each potential hazard were identified jointly by the system safety engineer and the appropriate design or operations engineer. In considering what the effects might be, further subsystem failures or accidents which could result as a consequence of the hazard were considered. If a hazard could result from a subsequent, non-related, but credible failure, accident or personnel error, this was defined as an additional potential hazard.

Hazard Reduction

Requirements for reduction of identified hazards were made in accordance with the Hazards Reduction Precedence Sequence (HRPS) of NASA OMSF Safety Program Directive No. 1 - Revision A (SPD-1A). This called for an order of precedence in identifying requirements as follows:

1. Design for minimum hazard.
2. Safety devices.
3. Warning devices.
4. Special procedures.
5. Identification as residual hazards.

Residual hazards are defined as those for which safety or warning devices and special procedures could not be provided for counteracting the hazard. Consequently where requirements could not be identified which sufficiently reduced the potential effects of a hazard to an acceptably safe level, the hazard was identified as a residual hazard (No. 5 on the HRPS). Where enough information was not available from the Phase B analyses to ensure a satisfactory resolution of a safety situation, this was identified as an unresolved safety issue. Residual hazards and unresolved safety issues are summarized in the following sections of this report.

1.3 RESIDUAL HAZARDS

The last step in the hazard reduction precedence sequence is the identification of residual hazards, those hazards which have not been eliminated by alternate designs or have not been reduced to insignificance by safeguards.

For example, cryogenic liquid is no longer a hazard because that form of hydrogen, oxygen, or nitrogen has been eliminated from the design. However, the presence of high pressure, gaseous hydrogen remains a hazard because of the potential flame and explosion effects when mixed with normal MSS atmosphere. Double containment reduced the hazard to manageable limits, but did not eliminate the hazard from further consideration. Section 2 of this report analyzes hazards identified in the MSS Safety Study. Residual hazards are summarized below:

- Leakage of hydrogen gas inside habitable volumes resulting in increased flammability and explosion potential.
- Rupture of high pressure tanks with subsequent shrapnel.
- Rupture of module pressure shell resulting in decompression.
- Breakup of control moment gyro rotor or support.
- Susceptibility of IVA and EVA pressure garment to tearing on protruding components.
- Fouling of long IVA hoses on internal components or structure.
- Inability to detect a toxic atmosphere or contaminated food.
- Leakage of external seals, particularly in hatches.
- Residual pressure differential across opening or closing hatches.
- Collision of crewman with sharp equipments during EVA/IVA.
- Fire.
- Meteroid penetration.
- Electric shock.
- Sudden release of station module pressure inside a closed shuttle cargo bay.
- Damage to station module or shuttle during berthing and docking.

1.4 UNRESOLVED SAFETY ISSUES

Residual hazards which are susceptible to additional study and experimentation have been defined as unresolved safety issues. The issue remains a hazard but advancement in the state-of-the-art can be immediate and positive in hazard resolution. Further design and safety efforts in these fields would be most productive in achieving safety goals. A summary of unresolved safety issues identified in the MSS safety analysis follows:

Fire Suppression: Sufficient data are not now available to assure the adequacy of any fire suppression system selected. Data are required on fire propagation characteristics, fire detections methods, and the effectiveness of fire suppression techniques, all under zero-g conditions. The Skylab program is probably the best but not the only means by which data may be collected for a rational decision. Combustion analysis and special experiments should be made prior to, concurrently with, and subsequent to the in-orbit tests. These results affect all manned space vehicles.

Pressurized Tanks: Some of the pressurized fluid tanks on the station, (station modules, cargo modules, and power boom) have a high TNT explosive equivalent; e.g., hydrogen and oxygen storage and accumulator tanks, the oxygen emergency supply tanks, and the nitrogen repressurization tanks. Explosive rupture of any one of these could be catastrophic. Continued attention is therefore required so as to ensure that adequate factors of safety, testing, and in-flight monitoring are provided and that the tanks are designed and located so that rupture will not destroy or damage the station. At present, a tank design is not available that has been demonstrated to fail so as to direct fragments and gases in a predeterminted direction. Fragment prevention is mandatory for safe operation, and could be achieved by adequate information about fracture mechanics, pressure cycling effects, long life stress effects and design methods which produce tank wall opening without releasing fragments.

Collision with Space Debris: The possibility exists that enough debris from U.S. and foreign spacecraft may be in intersecting orbits with the station to pose a significant hazard probability for a ten-year operation. A better analysis than is presently available is required to determine the probability of such a collision, and the relative impact velocity. If this is, indeed, found to be a significant hazard, then means should be evaluated to detect, track, and predict the paths of such debris; and to provide means for either removing individual items from collision orbits by the shuttle or other vehicle, or to provide some means of evasion by providing adequate and timely delta-V capability at the station.

Shuttle Emergency Capability: Emergency provisions are being provided on the station for 96 hours, based on the guideline constraint which calls for 48-hour shuttle capability to rendezvous. The additional 48 hours is provided for docking, transfer of personnel/cargo, and contingency margin, or for a second shuttle, if necessary.

Since the safety on the station is contingent on the worst-case shuttle emergency rendezvous and docking time, the shuttle capability in this respect should be periodically reevaluated throughout the program. Should the worst case exceed 96 hours, the station safety provisions must be reevaluated and updated.

Accidents: There are a number of potential accidents which could lead to personnel loss. A continuing effort is therefore required to reduce the probability of these accidents, to minimize the injury and damage they can cause, and to provide longer-term means for damage containment and control. Among these accidents are fire, explosion, and meteroid penetration.

Sudden Release of Station Module Pressure: The shuttle cargo bay will be vented to ambient. A maximum differential pressure will be determined for closed cargo bay-structural strength design. Inclusion of a pressurized station module in the cargo bay presents a hazard to the assembly because sudden release of the normal pressure would tend to overpressurize the cargo bay. Additional study of launch and reentry transients will be required to select a means of reducing this hazard.

Docking/Berthing: Where large inertias are involved, as between the shuttle and a module, small errors in closing rate, direction, or location could result in critical damage. Manual docking/berthing depends on human performance as well as on mechanical system response. Continued study of the docking/berthing procedure is necessary to identify the practical safeguards to preclude accelerations outside design tolerances.

Toxic Environment Detection: Long periods of unmanned operation could allow accumulation of toxic gases in the habitable module atmosphere. Detection means for all possible contaminants have not yet been applied to the manning operation. Several approaches should be taken; e.g., investigation of possible contaminants and identification of a set of sensors, or modification of the procedures to eliminate the contaminant buildup possibility.

Hatch Operation: Small pressure differences over a large hatch area could result in hatch accelerations dangerous to the crew and adjacent equipment. Continuing design detail is required to preclude this hazard.

2.0 HAZARDS

A number of sources were used to identify the inherent and potential hazards in the MSS.

1. Results of Space Station Program, Phase B.
2. Hazards arising from equipment failures.
3. Hazards inherent in normal and contingency operations.
4. Credible accidents, defined without specifically determining the cause.

The Phase B S-V Launched Space Station had many of the same characteristics as the MSS, and some already identified hazards applied to the modular design. Life support must still be supplied, as well as RCS attitude control and secondary electrical power. Even though cryogenic hazards have been eliminated, both hydrogen and oxygen gases are required for the engines and fuel cells. Applicable hazards were also identified by reviewing the hazards checklist formulated from a survey of applicable documents, including the NASA/MSC Space Flight Hazards Catalog.

Hazards were also identified from critical failures listed in the Critical Failure Analysis performed by reliability. These considered failures of equipment to the assembly level and identified hazards according to the possible effects of the failures: applying to personnel and/or system. The criticality levels did not deter the classification of a failure mode as a hazard, because a hazard could exist concurrent with multiple redundancy.

Additional hazards were identified by a review of the planned MSS operations. Both the hazards inherent in the normal operations and the potential hazards that would arise in the event of a failure to perform the desired operations were defined.

Since the critical function analyses and other sources of hazards have not considered potential situations (not within human control) arising from unexpected natural or induced environments, from system failures, or events such as collision with meteroids or space debris, potential accidents were identified separately. Each of the 17 identified in Section 2.3 were utilized in providing configurational and operational requirements for crew survival. Immediately following any unavoidable damage to or loss of equipment, provisions were made.

1. to prevent (further) loss of personnel
2. to contain the damage
3. to control the situation (restore to safe conditions), and
4. to provide for restoration of the normal operating condition.

The accidents were defined so that they were severe enough to impose design and operational requirements within credible limits. No credible accident was eliminated from consideration because the design consequences were too severe.

Hazardous equipment and dangerous materials were summarized from the previous hazards lists. Equipment was considered hazardous when failure of that piece of hardware resulted or when normal operation could result in injury to personnel or system damage. A valve failing open or closed is not hazardous, but a valve exploding is a hazard. Dangerous materials were identified if the potential for fire, toxicity, explosion, or corrosion were increased significantly. Thus, oxygen was not identified as corrosive but was listed as increasing the flammability. Inherent hazards were also identified; e.g., sharp corners on tables and chairs since failure of the hardware is not necessary to cause loss of personnel.

2.1 SUBSYSTEM HAZARDS

The hazard identification contained within this section delineates potential hazardous Modular Space Station subsystem failures and operational conditions which may endanger personnel or lead to damage or loss of equipment. The subsystem hazards which have been identified emerged from evaluation of the Modular Space Station subsystem critical functions and subsystem equipment implementing these functions.

Table 2.1-1 lists the potential hazards that have been identified from the Criticality I and II failure modes as determined by the Critical Function Analysis. The resulting potential hazard effects associated with each failure occurrence is indicated as leading to injury or to loss of personnel, or damage to or loss of equipment.

2.2 HAZARDOUS OPERATIONS

Hazardous operations are defined as those operations during which personnel errors, minor accidents or equipment failures could lead to injury to personnel or damage to equipment. Nonhazardous operations are those which are tolerant to personnel errors, minor accidents or equipment failures, i.e., do not result in injury to personnel or damage to equipment.

Personnel errors to be considered are errors such as operating the wrong switch, operating switches in the wrong sequence, omitting to operate a switch when required, misunderstanding a displayed instruction or verbal communication, operating valves in the wrong direction, etc. Personnel error does not mean gross operational errors such as inadvertently depressuring, dumping computer data, docking at 10 feet per second.

Minor accidents refer to bumping into sharp corners, spilling chemicals, breaking tools, breaking lamps, etc. It does not refer to the "credible accidents" which are considered major accidents and which are defined for separate consideration.

Table 2.1-1. Subsystem Hazards

Subsystem Hazard	Effect	Discussion
1.0 STRUCTURES & MECHANICAL		
1.1 PRIMARY STRUCTURE		
1.1.1 Rupture, fracture or puncture of primary structure (sidewall, airlock and berthing/docking bulkhead)	Rapid module decompression for a large hole resulting in loss of personnel in module or station and great difficulty to repair.	Design features to minimize those effects, including protective shields inside as well as outside of the pressure shell. However, the hazard of the single shell rupture is still possible, even with the relativ ely large factor of safety. A shall design which prevented the tearing of a smaller hole could further reduce the hazard. Rapid release of module atmosphere into the closed shuttle cargo bay could result in the loss of the shuttle, due to overpressure of the shuttle structure.
1.1.2 Structural failure of module support fitting	Impact of the module inside the shuttle cargo bay, with subsequent damage to the shuttle as well as module loss.	Most damage during launch and reentry. In addition to the three hard mounting points now envisioned, a few soft mounts would prevent large movements. Current design is considered adequate because of large safety factors.
1.2 SECONDARY STRUCTURE		
1.2.1 Failure of hatch seal	Continuous atmospheric leakage to space with subsequent shortening of on-orbit time or module abandonment.	These redundant seals are not maintainable in orbit. Module-to-module seals are designed for mission duration with only one assembly and no subsequent disturbance.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
1.2.2 Leakage of the flexport	Loss of atmosphere in the flexports affecting usage in emergency.	Safety proposes to keep the flexport hatches closed during operations (Section 4.2), reducing the effect. Normal operation of the station can continue until the passage can be repaired or replaced.
2.0 ENVIRONMENTAL CONTROL LIFE SUPPORT		
2.1 GASEOUS STORAGE		
2.1.1 Rupture or explosion of high-pressure (3000 psi) H_2, O_2 or N_2 storage tanks	Shrapnel and pressure wave release could injure personnel and damage module.	All configurations have included this hazard. Section 4.5 discusses safe means for reducing the effects. In the MSS, the high pressure tanks are placed in normally uninhabited modules. Continuing research on non-frangible tanks is necessary for maximum station safety.
2.1.2 Leakage of H_2 storage tank pressure control components or plumbing	Increasing H_2 content of the atmosphere could result in explosion or fire.	In zero-g, hydrogen will diffuse throughout the station. An ignition source anywhere could cause severe damage. Extraordinary measures must be taken to prevent leakage. For the MSS, the solution has been to provide double walled containment for hydrogen vessels and lines. Any leakage would be detected by pressure rise in the intermediate volume, and dumped overboard.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
2.2 CO_2 MANAGEMENT		
2.2.1 Degraded trace contaminant filtration	Injury to personnel by atmospheric contamination.	Gradual loss of contaminant filtration could have a gradual effect on the crew. However, warning of known contaminant buildup is provided by monitors.
2.2.2 Leakage of H_2 or CH_4 from Sabatier reactor	H_2 of CH_4 in module atmosphere could reach flammable or explosive mixtures.	CH_4 is also an efficient fuel. The discussion under 2.1.2 applies.
2.2.3 Leakage of H_2 from electrolysis units	Increasing H_2 content of the atmosphere could result in explosion or fire.	(See 2.1.2)
2.3 THERMAL CONTROL		
2.3.1 Leakage of freon from heat rejection loop	Increasing concentration of freon in the atmosphere could result in loss of personnel.	Freon is used for the external heat exchangers. Internal piping is double contained. Any leakage is detected and dumped overboard. Careful design of the venting system must prevent direct leak of atmosphere to space.
2.4 WASTE MANAGEMENT		
2.4.1 Leakage of liquids and waste	Equipment could be corroded and air contaminated for personnel.	Corrosive wastes could damage normal equipment, especially during the long time of expected operation. Low pressure and continuous processing of small quantities minimize the effects.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
3.0 ELECTRICAL POWER		
3.2 SECONDARY POWER GENERATION		
3.2.1 Rupture of O_2 EPS accumulator tanks (3000 psi during pre-manned operations and 300 psi when manned)	Both personnel and equipment could be lost.	During buildup, the energy is high enough to cause extensive damage to the core module, and to the shuttle during delivery. During manned operation, the tanks are operated as accumulators at 300 psi and are sized to prevent module/station overpressure, and the factor of safety is very large.
3.2.2 Leakage of H_2 accumulator tanks, feed plumbing, or components	Gradual H_2 concentration increase with possible explosion or fire.	See discussion in 2.1.2.
3.2.3 Rupture or explosion of 3000 psi H_2 or O_2 storage tanks	Shrapnel and pressure shock could be damaging to personnel, modules, and shuttle.	Placement in the power module minimizes the effects on the station. See 2.1.1 discussion.
3.2.4 Leakage of H_2 from fuel cell	Increased H_2 concentration in the atmosphere with possible explosion or fire.	See discussion in 2.1.2.
3.2.5 Leakage of H_2 from electrolysis units	Increased H_2 concentration in the atmosphere with possible explosion or fire.	See discussion in 2.1.2.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
3.3 ENERGY STORAGE		
3.3.1 Battery leakage of toxic gases or corrosive contaminants	Hydrogen leakage could cause local, explosive concentrations and battery electrolyte could leak and corrode surrounding equipment.	Effects are minimized by several safety features: batteries are used in the unmanned configuration only. Batteries are small compared to the module volume; i.e., any gas leak would not increase the total concentration to the flash point. Each battery is doubly contained, each wall being able to withstand the expected pressure increase with an additional safety margin.
4.0 GUIDANCE AND CONTROL		
4.4 MOMENTUM EXCHANGE		
4.4.1 Breakup of control moment gyro rotor or support equipment	Release of momentum in the pieces of rotor as shrapnel.	Containment of the rotor in a heavy shield would severely penalize the weight of the station. The alternative of providing large safety margins for the mounting was chosen as acceptable.
5.0 REACTION CONTROL		
5.1 PROPELLANT ACCUMULATORS		
5.1.1 Rupture of 300 psi H_2 or O_2 accumulator tank	Shrapnel and pressure wave could jeopardize personnel and equipment.	The safety margin of these tanks at the 300 psi level is very high, because of their use at 3000 psi during the unmanned buildup.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
5.1.2 Leakage of H_2 accumulator tanks or tank fittings	Increased H_2 concentration in the atmosphere with possible explosion or fire.	(See 2.1.2 discussion).
5.2 PROPELLANT FEED		
5.2.1 External leakage of propellant feed plumbing or components	Increased H_2 & O_2 concentration in the habitable atmosphere.	Since hydrogen causes the most severe effect, the hydrogen lines have been double enclosed to prevent leakage into the habitable atmosphere. Oxygen leakage increases the flammability of the atmosphere but sensors would indicate an out-of-tolerance condition before a severe change occurs.
5.3 ENGINE		
5.3.1 Explosion of a thruster	Shrapnel could damage the core module shell and personnel located in the core module.	Current thruster design has reduced this hazard sufficiently for the MSS. The amount of gaseous H_2 and O_2 in the chamber that is possible, is very small. Even at 50 psia (when firing), the small chamber would have very little energy as shown by Figure 4.5-1.
6.0 INFORMATION SUBSYSTEM		
(No hazards identified)		
7.0 CREW HABITABILITY		
7.2 GENERAL/EMERGENCY EQUIPMENT		

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
7.2.1 Degraded operation of emergency O_2 face mask	Personnel loss during an emergency.	Degraded operation during emergency is compensated for by the inclusion of redundant face masks in each isolatable volume. Only a short time (emergency duration) is involved; so the probability of failure is small. A regular maintenance inspection is mandatory.
7.2.2 Pressure garment tear or pressurization failure	Personnel loss during suited IVA and EVA.	Detailed design of the MSS must eliminate sharp corners (both inside and outside) or place protective barriers around necessary sharp shapes. Astronaut mobility is impaired with the current suit design; so every effort must be made to reduce the hazard during suited operations. Loss of pressurization without tearing is unlikely since the residual oxygen in the suit should allow sufficient time for entry into an airlock.
7.2.3 Malfunction of portable life support system during EVA	Personnel loss during EVA.	PLSS design must provide alternate means for allowing an astronaut safe return to an airlock. The "buddy" system is mandatory.
7.2.4 Malfunction of IVA umbilical connections and hoses during IVA operations	Personnel loss during suited IVA.	Trailing of umbilical lines inside a depressurized or toxic atmosphere module requires careful control of the positions of the lines. Entanglement with equipment or structure could limit the range of the suited astro-

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
7.2.4 (Continued)		naut and could prevent oxygen supply from reaching the suit. The "buddy" system provides rescue, capability and the suited astronaut should be able to reach the airlock with the unbilical disconnected.
7.3 FURNISHINGS		
7.3.1 Structural failure of crew mobility aids and restraints	Personnel injury	Failure of a mobility hand hold could result in stability loss of a moving astronaut with subsequent impingement on furniture corners. Loosening of restraints when sleeping could allow free floating and impingement. Redundant ties to structural members and a rigorous safety inspection will be necessary.
7.3.2 Structural failure of crew seating and seating restraints	Injury to personnel.	Inadvertent release of a seated astronaut could produce uncontrolled motion in a constrained position. However, redundant attachments to structure reduces the hazard and station acceleration are small.
7.3.3 Toxic refrigerant leakage from freezer or refrigerator	Incapacitance of personnel.	A buildup of refrigerant in habitable volumes could require temporary abandonment of the module and, at worst, loss of crew from atmospheric contamination. However, the quantity in the MSS is relatively small and the crew can detect leakage by mechanical sensors and by odor before severe effects occur. Double containment is in order.

Table 2.1-1. Subsystem Hazards (Cont)

Subsystem Hazard	Effect	Discussion
7.3.4 Malfunction of microwave oven	Injury to personnel.	Release of microwaves into habitable volumes in sufficient strength to cause crew injury is prevented by shielding. Inadvertent entry into an operating oven is prevented by an interlock for door opening. In addition, a signal light indicating open operation will warn the crew.

Equipment failures refer to component failures, i.e., IFRU failures - not failures of a complete assembly or subsystem. Component failures have been identified and analyzed by conducting critical failure analyses (DRL 68, Vol VI). In this report, equipment not directly associated with the MSS major subsystems (i.e., shuttle manipulator arms and shuttle docking) are included in the analysis of hazardous operations.

Table 2.2-1 identifies hazardous operations by mission phase.

2.3 CREDIBLE ACCIDENTS

Since the critical functions analysis and other sources of hazards do not, in general, consider potential situations arising from unexpected natural or induced environments, gross system failures, or events, such as collision with meteroids or space debris, which are not within human control, it was found necessary to identify and define potential accidents that may occur on or to the space station, and for which it is desired to provide design and operational features for crew survival. Identified credible accidents are as follows:

a. Fire - A fire in an area containing subsystems equipment, electrical wiring or laboratory equipment, which damages and puts out of commission all unprotected operating equipment in a compartment. A compartment, for this purpose, is a space which can be closed off by doors and hatches, but which need not be airtight or pressure tight. Flame propagation will be confined to the one compartment. Sufficient smoke/fumes will be produced to require rapid evacuation of the affected compartment by personnel. Personnel in other areas will be able to continue normal operations, but will require face masks to enter the affected area. The opening of hatches and other openings to the affected area will be minimized for 24 hours, while fumes are present. Electrical cable, service conduits, plumbing lines and ducts may temporarily become inoperative (e.g., power will be removed from electrical cables, fluid transfer will be interrupted, etc.) but will not be affected by the fire if they were designed for fire protection, and will be brought on-line again after a system checkout, within approximately an hour. Similarly, operating equipment specifically designed for protection from fire will be temporarily inactivated, but will be brought on-line again after checkout.

b. Mechanical Damage - Mechanical damage caused by a collision inside the vehicle with loose out-of-control masses. A momentum equivalent to a 50-pound mass moving at 2 ft/sec will be involved. The collision may occur with any equipment which is exposed to a collision path (i.e., no intervening equipment) of approximately five feet or more, but not to primary structure. The damage will be confined to the equipment within a two-foot radius of the impact point. All equipment, cables, fluid lines, ducts, etc., will be damaged and put out of commission until they can be repaired/replaced except equipment which is specifically armored for protection against collision.

Table 2.2-1. Hazardous Operations

Hazardous Operation	Effect	Discussion
1. Launch to orbit.	Loss of station module, shuttle, and shuttle personnel.	Launch of a space vehicle constitutes a hazardous operation in a space mission because of precise operational requirements of many systems and crew in a limited time period. Any shuttle loss also loses the cargo and inability of the shuttle to orbit may require jettison of the cargo in order for the shuttle to land safely. In addition, specific malfunctions in the station module could result in shuttle loss; e.g., module support breaking or rapid release of module atmosphere into the cargo bay.
2. Docking.	Loss of station personnel, station modules, shuttle, and shuttle personnel. Loss of ability to dock to station.	While berthing of modules to the station by means of a shuttle manipulator constitute the normal operating mode, direct docking remains a safety consideration since it constitutes a backup mode as well as the mode for connecting a free flying module. Major hazards arise from the potential of puncturing or damaging structure of the station or module, damage to the docking mechanism or loss of seal integrity. Uncontrolled closing is prevented by means of redundant controls in shuttle and station. Either can control relative motion between the module and station. An alternate docking port on the station is required to provide backup capability in the event of a damaged port or mechanism. Terminal guidance by mechanical constraints should prevent relative motion that could damage the interface seals.

Table 2.2-1. Hazardous Operations (Cont)

Hazardous Operation	Effect	Discussion
3. Berthing and unberthing of station, cargo module, and RAM.	Loss of station personnel. Loss of or damage to module. Damage to station or shuttle.	Berthing hazards result from shuttle manipulator operations and include uncontrolled contact between module and station or shuttle, and loss of manipulator capability with the module between the shuttle bay and the station docking port. Uncontrolled manipulator operation and minimized by redundancy of controls and the slow motion of the manipulator vehicle precludes high energy contact between module and station or shuttle. Loss of manipulator capability could preclude both station berthing and return to the shuttle bay necessitating jettisoning the module and the manipulator to permit safe shuttle return. A backup docking port on the station is required to insure emergency access from the shuttle if the primary berthing port is damaged or inoperable.
4. Activation of station and cargo module.	Personnel loss from undetected hazard in unmanned module.	Detection of all possible atmospheric contaminants is difficult in zero-g but is essential for crew safety. The module is monitored for flammable gases while in the shuttle bay and safety requires that initial entry to a station module after an unmanned period (e.g., during buildup) should probably be conducted IVA to permit atmospheric sampling.
5. Opening & closing of module hatches.	Loss of personnel and equipment from rapid hatch motion.	Retention of a pressure differential across a hatch before opening could accelerate the hatch rapidly. Crew and equipment in the path could be injured and damaged. Section 4.6 discusses this hazardous operation. However, adequate safeguards can be incorporated into the detail design by multiple $\triangle P$ measurement, pressure equalization and mechanical restraints.

Table 2.2-1. Hazardous Operations (Cont)

Hazardous Operation	Effect	Discussion
6. EVA	Loss of personnel.	Hazards associated with EVA include loss of viable atmosphere due to a suit or PLSS leak, astronaut strain in physical activity and inability to return to the station. Loss of atmosphere can range from slow leaks or failure in the PLSS to massive leaks due to tearing large openings in the suit. This hazard is minimized by multi-layered suits and station design to avoid points and sharp corners and significant body functions are continuously monitored. Safety requires use of the "buddy" system and availability of EVA airlocks to facilitate rescue. All EVA operations should be performed on a tether to preclude unrecoverable separation from the station.
7. IVA	Loss of personnel from suit or umbilical damage.	Maneuvering in small volumes with a suit and umbilical in zero-g will be very difficult. Protection from sharp corners is necessary. Umbilical tangling must be prevented. As with EVA, the "buddy" system facilitates rescue. Retention of sufficient oxygen in the unconnected suit to allow return to the airlock is possible.
8. Module unberthing/shuttle undocking operation.	Loss of equipment. Loss of pressure.	Inability to separate the shuttle from the station at the docking ring results in the loss of the shuttle to further use. Redundant separation means must be provided. Inability to unberth a cargo module prevents reuse and reduces the number of potential docking ports. Station storage can still be provided. Provision should be made for unberthing from either end of the berthing adapter.

Table 2.2-1. Hazardous Operations (Cont)

Hazardous Operation	Effect	Discussion
9. Descent.	Loss of payload module, shuttle personnel, and shuttle.	Reentry accelerations generate large forces for breakage in the station module. All components must be attached or stowed securely. A careful inspection before cargo bay insertion must be made to insure no loose equipment. Certain specific component failures could lose the entire assembly; e.g., structural attachment of the module to shuttle and release of module pressure into the shuttle cargo bay.
10. Galley Operation.	Personnel injury.	Food preparation involves cutting, heating, and cooling operations. All of these processes are dangerous to human tissue. In addition, release of liquids and solids could overload the environmental control system as well as clog or corrode exposed operating components. Special equipment and operating techniques will be necessary to insure safety. Contamination and spoilage of food must be avoided or detected.

c. Explosion - An explosion of .025 pound TNT equivalent, releasing 50 BTU of energy in the form of heat, shock waves and kinetic and thermal energy of shrapnel damage will be confined to one compartment and will consist of overpressure, heat shrapnel and atmospheric contaminants. All equipment in the compartment will be damaged and made inoperative unless armor-plated against this type of explosion. The equipment will require repair/replacement, depending on the damage such an explosion can produce. Further hazards which can result in the compartment by such an explosion, such as fire, etc., should also be considered as part of this accident. Walls and primary structure, or equipment outside the affected compartment, will not be damaged.

d. Loss of Pressurization - A loss of pressurization in a module caused by an accidental penetration of an outside wall or bulkhead, by a faulty relief valves, or by a leaking pressure seal. The time from detection of the failure to reaching a nonhabitable environment will be approximately (TBD) corresponding to a 2-1/2 inches diameter hole. This accident may require evacuation of the affected pressure isolatable volume and the subsequent detection and repair of the source of leakage by two IVA personnel. No equipment will be damaged by the accident itself, but since the whole of the affected pressure volume may be exposed to vacuum conditions, sensitive equipment may have to be deactivated to survive the period until repressurization.

e. Fluid Leakage - Leakage of any gas or liquid which is produced, stored or routed through the pressurized areas of the vehicle, including any chemicals used or that may be produced in experiments. The leakage may occur at any point through which the fluid is routed. The amount of leakage will vary with the provisions made for detection and with the provisions for stopping the leakage (dumping the fluid overboard, shutting off the process, transferring to another tank, etc.). This quantity should be defined for every potentially hazardous fluid on-board. Following detection, the leakage may be confined to the affected area by restricting air circulation and providing a slight dump to vacuum in that area. Damage to equipment (e.g., from corrosion, etc.) and the possible requirement to temporarily evacuate the area must be considered separately for each on-board fluid.

f. Collision - A grazing collision with another vehicle or with space debris which damages equipment outside the spacecraft such as RCS jets, radiators, solar panels, antennas, tanks, fluid lines, docking mechanisms, etc. The collision is not severe enough to cause a penetration of primary structure, but may damage exposed equipment over a circular area of approximately three-foot diameter in any module or the solar array structure. The damage will require maintenance/repair/replacement to restore the function. If the equipment is not maintainable/repairable/replaceable, the damage is to be regarded as permanent.

g. Personnel Loss - The loss of any one man through injury, illness, or death. Provisions must be made for medical treatment until his return to earth, and for cross-training to allow other personnel to take over duties necessary for crew safety.

h. Food or Water Contamination - Biological or toxic contamination of food or potable water supply. All similarly packaged food stored in any one module will be assumed unfit to eat. Similarly, all potable water in connected tanks will also be assumed toxic; the water, however, may be reprocessed through the water purification system and the tanks decontaminated to render it potable.

i. Accident in a Hatch - The loss of access to any one hatch assembly, door or other personnel or cargo transfer opening because of jamming of the mechanism, either open or closed, or because of obstruction by cargo, or because of a localized hazardous situation (fire, chemical spillage, electrical hazard, etc.). The hazardous or non- accessible area may extend over a volume of about 5 ft x 5 ft x 5 ft and be situated anywhere within five feet of the edge of the hatch or opening.

This accident is not to be considered credible where two independent methods for opening a hatch have been provided and where special provisions have been taken to avoid hazardous equipment in the vicinity of the hatch.

j. Incapacitated EVA or IVA Man - An out-of-control and incapacitated man performing EVA or IVA. Rescue is required within five minutes by a companion already suited and conditioned to the suit atmosphere, who is waiting in an airlock or is also performing EVA or IVA.

k. Meteroid Penetration - Meteroid penetration of the primary structure. The results will be similar to an explosion, as described in item c, releasing 50 BTU of energy. Such a meteroid has a 10^{-3} probability of impact in 10 years, and the meteroid is approximately 0.6-inch diameter. Physical damage will be confined to one compartment (see definition if item a), and will consist of finely divided molten high-speed shrapnel (from spallation of the inner wall). All equipment in the compartment will be damaged and made inoperative, unless armor-plated for protection against this type of shrapnel. Damaged equipment will require extensive repair/replacement. Further hazards which can result in the compartment by such an accident, such as fire, etc., should also be considered as part of this accident. The resulting penetration of the pressure wall will be 2-1/2 inches in diameter and will cause depressurization of the vehicle to an unsafe level in approximately (TBD).

l. Loss of Electrical Power - Loss of the availability of electrical power from like power sources (all solar panels, or all fuel cells, or all batteries) in one pressure volume or all inverters in one volume, as the result of an accident and/or a sequence of unexpected failures. The loss will be immediate with no advanced warning.

m. Atmospheric Contamination - Atmospheric contamination by toxic or otherwise hazardous contaminants that will require personnel evacuation from one pressure isolatable volume within two minutes of detection. The affected volume will require either purging to vacuum and subsequent pressurization or, if the contaminant can be removed by the ECLSS, will require processing of the atmosphere for two days to restore a habitable environment. The other pressure volume will remain habitable.

n. Electrical Shock - Electrical shock to any one man while performing maintenance or working with electrical or electronic equipment or experiments. The shock may result in momentary (seconds to minutes) loss of performance capability by the man, to injury to the man's emergency return to earth, and/or loss of life.

o. Hazard in a Docked Module - A hazard appearing on a docked cargo, experiments or other module, which arises from any of the above accidents occurring on the module, as applicable. The module is to be considered as a separate pressure volume from the point of view of isolation, containment and control. If required, access to a depressurized or contaminated module will be by two IVA or EVA personnel.

p. Module Abandonment - A combination of accidents and/or equipment degradation requiring the return of any one module to earth for repair or replacement. The crew must operate in the remainder of the station at a reduced level until the module can be replaced on the station.

q. Station Abandonment - A combination of accidents and/or subsystems degradation requiring the abandonment of the station by some of all of the occupying personnel. Such abandonment will not be a time-critical emergency, but a deliberate abandonment planned over a period of days to months. The worst design case is when one of the separate pressure volumes has been evacuated and sealed off for up to 30 days because of major damage or contamination, and all personnel are in the remaining volume. Furthermore, subsystems degradation is now becoming apparent in this volume, resulting in the decision to abandon; such subsystems as are capable of survival must be set in a passivated or quiescent mode to ensure safe personnel escape and to minimize damage for possible reoccupation at a later date.

2.4 HAZARDOUS EQUIPMENT

This section contains a list, Table 2.4-1, of hazardous equipment identified for the station's major subsystems. The potential hazards associated with this equipment can be the result of normal operation as well as abnormal operation. Hazardous equipment is identified by any one of the following characteristics:

1. Equipment that contains sufficient releasable energy (kinetic, potential, pressure, thermal, chemical, etc.) to cause injury to personnel or damage to equipment if release at normal or maximum possible rates. Examples are a high-pressure hose and the docking operation. These contain enough energy to injure personnel or damage equipment even though it takes certain failures and/or accidents, credible or incredible, to release the energy and do the damage.

2. Equipment that contains or has the potential for producing toxic materials, corrosives, radiations, or environments, in concentrations which are injurious to personnel or equipment. Examples are RCS using hydrogen (explosive) and electrical equipment (electric shock). Again "how" the material or environment is released, or its credibility, is not considered in determining what is and what is not hazardous equipment.

3. Equipment that has the potential of triggering off a high-energy release or the production of toxic materials, corrosives, radiations or injurious environments. Examples are electrical equipment (ignition source), chisel-like tools and implements (can penetrate pressure walls).

Table 2.4-1. Hazardous Equipment List

Hazardous Equipment	Potential Hazards
1. Gas storage accumulators	Rupture of pressure vessel (Energy equivalent to approximately .08 lb to 6.5 lb of TNT per accumulator)
2. Water electrolysis unit	Leakage of combustible gas (H_2)
3. Fuel cell	Leakage of combustible gas (H_2)
4. Thermal control (freon) loop	Leakage of toxic gas (Dichlorofluoromethane, Freon 21)
5. Fire extinguishers	Rupture of pressure vessel (CO_2)
6. Control moment gyros	Breakup of rotor or failure of support attachment
7. H_2O tanks	Equipment damage caused by uncontrolled release of H_2O
8. Sabatier reactor	Leakage of combustible and toxic gas (CH_4)
9. Freezer/refrigerator	Leakage of toxic gas (Freon)
10. Microwave oven	Radiation leakage Crew injury from interlock failure and crew error
11. IVA/EVA pressure suit	Pressure decay from suit damage

Table 2.4-1. Hazardous Equipment List (Cont)

Hazardous Equipment	Potential Hazards
12. PLSS	Loss of oxygen content
13. Emergency O_2	Rupture of O_2 storage vessel or loss of oxygen content
14. Shuttle manipulator arms	Malfunctions of control/stop mechanism
15. Module pressure shell.	Rapid decompression During transport, shuttle cargo bay overpressurization
16. Module support structure in shuttle cargo bay	Launch or reentry forces could cause internal collision damage
17. High pressure gas storage	Explosion in power module or cargo module

2.5 DANGEROUS MATERIALS

Elimination of dangerous materials has been the goal in the MSS design. Notably, transport of water has been used to supply hydrogen and oxygen to the orbiting station. The products of electrolysis can be used in the reaction control engines and as the oxygen supply to the crew. Thus, transport and storage of a relatively common fluid under low pressure has decreased the need for high-pressure or cryogenic gas containers and has provided several sources for backup supply. The use of hydrazine in the RCS engines was rejected because of features necessary to contain the extra hazards involved with the toxic and explosive fluid.

Residual dangerous materials have been placed in double containers to reduce the hazard of leakage into habitable volumes and, where possible, have been located away from crew:

1. Freon for the external heat exchangers - Components internal to the station modules are double contained. The intermediate space between the component and the habitable volume can be vented to space. Freon is toxic to crew, but can be detected readily. Should the volume become contaminated, sufficient time is available for evacuation of the crew; and restoration of a habitable atmosphere can be accomplished by dumping of freon in that module and repressurization.

2. Hydrogen for the RCS from power module storage and from the electrolysis units - Components and lines internal to the station modules are double contained. Hydrogen concentration in a normal atmosphere results in an explosive or flammable mixture. Even though a source of energy must be supplied for ignition, the mixture is a potential hazard to personnel and hardware.

3. Vent gases from the Sabatier process contain methane - the entire vent system is double contained. Release of methane is toxic and flammable but readily detectable.

Additional dangerous materials have not been considered hazardous enough for double containment, but have been carefully contained and controlled.

1. Oxygen for the RCS and for the crew atmosphere - Increasing the concentration of oxygen in the habitable atmosphere increases the susceptibility of normal materials to fire. However, the presence of nitrogen continues to be a diluent and fire retardant within detectable pressure increases. Redundant means of oxygen content measurement will provide early detection of any problem.

2. Urine from the crew - The corrosive ability of urine is well known. The extended time necessary to accomplish significant damage to exposed equipment (particularly, electrical connectors) is available because of the expected duration of the MSS mission.

3. Potassium hydroxide for fuel cell operation - This caustic compound is damaging to human tissues, but release is very unlikely since containment is provided in individual cans; i.e., no handling of potassium hydroxide outside of the can.

Many materials have not been considered hazardous because of the MSS mixed atmosphere. A pure oxygen atmosphere would preclude such materials as teflon and rubber because of the flammability. Even in zero gravity, a residual flame continues (at least for the zero-g time experienced in airplane tests). This problem should be studied more completely.

3.0 SAFETY REQUIREMENTS

Safety requirements for the Modular Space Station were stated initially in the NASA Guidelines and Constraints document. These were reviewed and restated as general safety criteria in the System Requirements Book (SRB). As the study progressed, additional safety criteria and design requirements were developed and published in the SRB. They appear in final form in Section 3.1 of this report and are documented in Section 3.1.3.7 of DRL 66, Preliminary Performance Specification. Specific subsystem safety design requirements are listed in Section 3.2 of this report and are documented in the various subsystem sections of DRL 66.

3.1 SAFETY CRITERIA

Safety is a mandatory consideration through the total program. As a goal, no single malfunction or credible combination of malfunctions and/or accidents shall result in serious injury to personnel or to crew abandonment of the space station.

A. Provisions shall be made for the protection and survival of the whole crew during solar storm activity as defined by the design mission radiation model (Paragraph 3.1.3.4, DRL 66). The radiation dosage limitations defined in Paragraph 3.1.1 C, DRL 66 shall apply.

B. Personnel escape routes shall be provided in all hazardous situations. A design goal shall be to provide alternate escape routes that do not terminate into a common module area.

C. The space station shall be divided into at least two pressurized habitable volumes so that any damaged module can be isolated as required. Accessible modules will be equipped and provisioned so that the crew can safely continue a degraded mission and take corrective action to either repair or replace the damaged module.

D. Provisions and habitable facilities shall be adequate to sustain the entire crew for a minimum of 96 hours during an emergency situation requiring shuttle rescue.

E. Atmospheric stores and subsystem capacity sufficient for one repressurization shall be maintained on/at the space station during manned operations to independently supply each pressurized habitable volume.

F. Access to EVA and IVA airlock suit station(s) shall be provided for all credible emergency conditions. Airlock chamber(s) shall be provided to permit crew access for EVA/IVA operations.

G. Two or more suited crewmen will participate in any pressure suit activity and rescue provisions will be provided.

H. The atmosphere constituents, including harmful airborne trace contaminants and odors will be monitored and controlled in each pressurized habitable volume.

I. Identified hazards shall be eliminated, reduced to controlled hazards, or specified as residual hazards.

J. Capability shall be provided for performing critical functins at an emergency level until the crew can be rescued, with any one pressure isolatable volume and the supplies and equipment within it unavailable. If the crew is divided into two or more pressure isolatable volumes which are not shirtsleeve connected, then each of these volumes shall be capable of sustaining the whole crew. Electrical and fluid lines in the affected volume required for critical functions shall be protected against the effects of explosion, fire, vacuum, and corrosion.

K. Capability shall be provided for performing critical functions with the portion of any one subsystem in one pressure isolatable volume inactivated as a result of an accident and a portion of the subsystem in the other pressure isolatable volume(s) inoperative for maintenance.

L. For those malfunctions and/or hazards which may result in time-critical emergencies, provision shall be made for the automatic switching to a safe mode of operation and for caution and warning of personnel.

M. Two or more entry/egress paths shall be provided to and from every module, pressure isolatable volume, or other area with restricted access. The two paths shall be separated by airtight partitions, or shall be at least 10 feet apart, and shall each lead to an area in which the crew can survive until shuttle rescue or resupply.

N. Provisions shall be made for detecting,containing (i.e., confining) and controlling (i.e., restoring to a safe condition) emergencies such as fires, toxic contamination, depressurization, structural damage, etc.

O. Primary pressure structural materials shall be non-flammable. Interior walls and secondary structure shall be self-extinguishing.

P. All continuous nonmetallic materials shall be self-extinguishing in the most severe oxidizing environment to which they will be exposed. Means shall be provided for fireproof storage of medical supplies, maintenance supplies, food, tissue, clothing, trash, and for other non-self-extinguishing items, when they are not in use.

Q. Materials used in the habitable areas shall not outgas toxic constituents in the lowest pressure environment to which they will be exposed.

R. Potentially explosive containers such as high pressure vessels or volatile gas storage containers shall be placed outside of and as remotely as possible from personnel living and operating quarters. Wherever possible the containers shall be isolated and protected so that failure of one will not propagate to others.

S. Redundant equipment, lines, cables, and utility runs which are critical for safety of personnel or mission continuation shall either be located and routed in separate compartments (i.e., separated by a structural wall) or shall be protected against fire, smoke, contamination, overpressure, and shrapnel.

T. All walls, bulkheads, hatches and seals whose integrity is required to maintain pressurization shall be readily accessible for inspection and repair by crewmen in pressurized suits.

U. All EVA and unpressurized compartment IVA shall be conducted using the "buddy system". The buddy system shall also be used during shirtsleeve operations in hazardous areas.

V. A margin of consumables shall be provided onboard, sufficient for performing critical functions for 96 hours at a reduced level following any credible accident which renders one pressure isolatable compartment unavailable.

W. The capability shall be provided on the space station for the detection of malfunctions and/or hazards, tracing to the failed replaceable unit and the display of information to the crew necessary for corrective action.

X. Range safety requirements at Kennedy Space Center and the Air Force Eastern Test Range shall apply. Waivers required to meet mission requirements will be identified.

Y. At least two egress paths shall be available from each module for emergency egress of personnel during manned ground operations.

Z. Emergency suits required in the space station core module shall be in readily accessible locations within each pressure isolatable volume.

AA. Provisions shall be made for emergency medical treatment for durations compatible with the rescue provisions.

BB. The safe environment and the safe operational status or activated subsystems within the space station shall be verified prior to personnel etnry, initially and prior to re-entry following temporary station abandonment.

CC. Deployment and initiation of operations considered hazardous shall be checked out from a safe location before exposing crewmen to the potential hazards.

DD. All EVA shall be conducted either using the "buddy system" or within visual range of a suited crewman ready to exit.

EE. Provision shall be made for the return of a crewmen incapacitated while performing EVA.

FF. Provisions shall be made for the containment and/or disposal of toxic contaminants.

GG. Provide containment of all materials requiring return via the shuttle to prevent contamination of the environment and reduce the hazard of potential fire and toxic conditions.

HH. Tanks used as gas accumulators in inhabited areas shall be designed to a factor of safety of 4.0 as a minimum. Tank supports shall be designed to restrain the tank under propulsive effect of rapidly escaping gas.

II. Design provisions shall be incorporated to prevent uncontrollable hatch opening due to pressure differentials.

3.1.1 Credible Accidents

The space station shall be designed and operated so that crew survival and station survival will be ensured following the accidents defined herewith.

A. Fire

A fire in an area containing subsystems equipment, electrical wiring or laboratory equipment, which damages and puts out of commission all unprotected operating equipment in a compartment. A compartment, for this purpose, is a space which can be closed off by doors and hatches, but which need not be airtight or pressure tight. Flame propagation will be confined to the one compartment. Sufficient smoke/fumes will be produced to require rapid evacuation of the affected compartment by personnel. Personnel in other areas will be able to continue normal operations, but will require face masks to enter the affected area. The opening of hatches and other openings to the affected area will be minimized for 24 hours, while fumes are present. Electrical cable, service conduits, plumbing lines and ducts may temporarily become inoperative (e.g., power will be removed from electrical cables, fluid transfer will be interrupted, etc.) but will not be affected by the fire if they were designed for fire protection, and will be brought on-line again after a system checkout, within approximately an hour. Similarly, operating equipment specifically designed for protection from fire will be temporarily inactivated, but will be brought on-line again after checkout.

B. Mechanical Damage

Mechanical damage caused by a collision inside the vehicle with loose out-of-control masses. A momentum equivalent to a 50 lb. mass moving at 2 ft/sec will be involved. The collision may occur with any equipment which is exposed to a collision path (i.e., no intervening equipment) of approximately five feet or more, but not to primary structure. The damage will be confined to the equipment within a two foot radius of the impact point. All equipment, cables, fluid lines, ducts, etc. will be damaged and put out of commision until they can be repaired/replaced except equipment which is specifically armored for protection aginst collision.

C. Explosion

An explosion of .025 lb TNT equivalent, releasing 50 BTU of energy in the form of heat, shock waves and kinetic and thermal energy of shrapnel damage will be confined to one compartment (see definition in Item A) and will consist of overpressure, heat, shrapnel and atmospheric contaminants. All equipment in the compartment will be damaged and made inoperative, unless armor plated for protection against this type of explosion. The equipment will require repair/replacement, depending on the damage such an explosion can produce. Further hazards which can result in the compartment by such an explosion, such as fire, etc., should also be considered as part of this accident. Walls and primary structure, or equipment outside the affected compartment, will not be damaged.

D. Loss of Pressurization

A loss of pressurization in a module caused by an accidental penetration of an outside wall or bulkhead, by a faulty relief valve, or by a leaking pressure seal. The time from detection of the failure to reaching a non-habitable environment will be approximately (TBD) corresponding to a 2-1/2 inches diameter hole. This accident may require evacuation of the affected pressure isolatable volume and the subsequent detection and repair of the source of leakage by two IVA personnel. No equipment will be damaged by the accident itself. But since the whole of the affected pressure volume may be exposed to vacuum conditions, sensitive equipment may have to be deactivated to survive the period until repressurization.

E. Fluid Leakage

Leakage of any gas or liquid which is produced, stored or routed through the pressurized areas of the vehicle, including any chemicals used or that may be produced in experiments. The leakage may occur at any point through which the fluid is routed. The amount of leakage will vary with the provisions made for detection and with the provisions for stopping the leakage (dumping the fluid overboard, shutting off the process, transferring to another tank, etc.). This quantity should be defined for every potentially hazardous fluid

E. Fluid Leakage (Cont)

onboard. Following detection, the leakage may be confined to the affected area by restricting air circulation and providing a slight dump to vacuum in that area. Damage to equipment (e.g., from corrosion, etc.) and the possible requirement to temporarily evacuate the area must be considered separately for each onboard fluid.

F. Collision

A grazing collision with another vehicle or with space debris which damages equipment outside the spacecraft, such as RCS jets, radiators, solar panels, antennas, tanks, fluid lines, docking mechanisms, etc. The collision is not severe enough to cause a penetration of primary structure, but may damage exposed equipment over a circular area of approximately three foot diameter. The damage will require maintenance/repair/replacement, to restore the function. If the equipment is not maintainable/repairable/replaceable, the damage is to be regarded as permanent.

G. Personnel Loss

The loss of any one man through injury, illness, or death. Provisions must be made for medical treatment until his return to Earth, and for cross-training to allow other personnel to take over duties necessary for crew safety.

H. Food or Water Contamination

Biological or toxic contamination of food or potable water supply. All similarly packaged food stored in any one module will be assumed unfit to eat. Similarly all potable water in connected tanks will also be assumed toxic, the water however may be reprocessed through the water purification system and the tanks decontaminated to render it potable.

I. Accident in a Hatch

The loss of access to any one hatch assembly, door or other personnel or cargo transfer opening because of jamming of the mechanism, either open or closed, or because of obstruction by cargo, or because of a localized hazardous situation (fire, chemical spillage, electrical hazard, etc.). The hazardous or non-accessible area may extend over a volume of about 5 ft x 5 ft x 5 ft and be situated anywhere within 5 ft of the edge of the hatch or opening.

This accident is not to be considered credible where two independent methods for opening a hatch have been provided and where special provisions have been taken to avoid hazardous equipment in the vicinity of the hatch.

J. Incapacitated EVA or IVA Man

An out-of-control and incapacitated man performing EVA or IVA. Rescue is required within 5 minutes by a companion already suited and conditioned to the suit atmosphere, who is waiting in an airlock or is also performing EVA or IVA.

K. Meteroid Penetration

Meteroid penetration of the primary structure. The results will be similar to an explosion, as described in Item C, releasing 50 BTU of energy. Such a meteroid has a 10^{-3} probability of impact in 10 years and the meteroid is approximately 0.6 inches in diameter. Physical damage will be confined to one compartment (see definition in Item A), and will consist of finely divided molten high speed shrapnel (from spallation of the inner wall). All equipment in the compartment will be damaged and made inoperative, unless armor plated for protection against this type of shrapnel. Damaged equipment will require extensive repair/replacement. Further hazards which can result in the compartment by such an accident, such as fire, etc., should also be considered as part of this accident. The resulting penetration of the pressure wall will be 2-1/2 inches in diameter and will cause depressurization of the vehicle to an unsafe level in approximately (TBD).

L. Loss of Electrical Power

Loss of the availability of electrical power from like power sources (all solar panels, or all fuel cells, or all batteries) in one pressure volume or all inverters in one volume, as the result of an accident and/or a sequence of unexpected failures. The loss will be immediate with no advanced warning.

M. Atmospheric Contamination

Atmospheric contamination by toxic or otherwise hazardous contaminants that will require personnel evacuation from one pressure isolatable volume within two minutes of detection. The affected volume will require either purging to vacuum and subsequent repressurization, or, if the contaminant can be removed by the ECLSS, will require processing of the atmosphere for two days to restore a habitable environment. The other pressure volume will remain habitable.

N. Electrical Shock

Electrical shock to any one man while performing maintenance or working with electrical or electronic equipment or experiments. The shock may result in momentary (seconds to minutes) loss of performance capability by the man, to injury requiring the man's emergency return to Earth, and/or loss of life.

O. Hazard in a Docked Module

A hazard appearing on a docked cargo, experiments or other module, which arises from any of the above accidents occurring on the module, as applicable. The module is to be considered as a separate pressure volume from the point of view of isolation, containment and control. If required, access to a depressurized or contaminated module will be by two IVA or EVA personnel.

P. Module Abandonment

A combination of accidents and/or equipment degradation requiring the return of any one module to Earth, for repair or replacement. The crew must operate in the remainder of the station at a reduced level until the module can be replaced on the station.

Q. Station Abandonment

A combination of accidents and/or subsystems degradation requiring the abandonment of the station by some or all of the occupying personnel. Such abandonment will not be a time-critical emergency, but a deliberate abandonment planned over a period of days to months. The worst design case is when one of the separate pressure volumes has been evacuated and sealed off for up to 30 days because of major damage or contamination, and all personnel are in the remaining volume. Furthermore, subsystems degradation is now becoming apparent in this volume, resulting in the decision to abandon, such subsystems as are capable of survival must be set in a passivated or quiescent mode to ensure safe personnel escape and to minimize damage for possible reoccupation at a later date.

3.1.2 Dangerous Materials and Components

A. Toxic fluid containers shall be located in unpressurized volumes, or shall be double contained with the capability of dumping the fluid to space or off-loading to another double container, and of venting the space between the two containers.

B. Double contained toxic fluid containers shall be provided with means to detect leakage of the toxic fluid into the space between the containers, and with means to detect penetration of the outside container.

C. Means shall be provided for detecting a toxic environment within a space station module containing toxic or potentially toxic fluids.

D. Special protective garments and equipment shall be provided for personnel working near potentially toxic MSS elements during ground handling or working in a toxic environment.

E. Capability shall be provided to purge or dump to space a toxically contaminated atmosphere in a pressurized module.

F. Hazardous fluids or materials will be double contained during handling and transfer in pressurized areas. Capability shall be provided to verify the integrity of both containers before and after transfer.

G. Capability shall be provided to vent the space between double walled containers for hazardous fluid handling to space and dumping the fluid to space or off-loading to another container.

H. Procedures shall be available for transferring hazardous fluids, or materials in a pressurized area from a singly penetrated double container to a storage container without releasing fluid or material to the MSS atmosphere.

I. During handling and transfer of hazardous fluids or materials, no other manned operations shall be planned along the transfer path.

J. The pressures, temperatures, or other parameters which indicate the status of hazardous fluids or materials shall be verifiable.

K. Transfer lines for hazardous fluids shall be located outside the pressurized vessels or shall be double walled with the capability of venting the space between the two containers to space.

3.2 SUBSYSTEM SAFETY REQUIREMENTS

3.2.1 General

A. Equipment in pressurized areas which is required for safety of personnel or mission continuation shall be capable of surviving, active or dormant, in a depressurized environment for a time period sufficient to ensure re-establishment of a pressurized atmosphere in a damaged volume, but in any case for a minimum of 48 hours.

B. Factors of Safety - The following factors of safety (Table 3.2.1-1) shall be used for structural design, applied to limit load:

Table 3.2.1-1. Factors of Safety for Structures

Condition	Factor of Safety	
	Ultimate	Yield
Unmanned	1.50	1.20
Manned		
Long-Term Sustained Loads	2.00	1.50
Short-Term Transient Loads	1.75	1.30

C. Limit Condition - No system shall be designed incapable of functioning at limit load conditions.

D. Fail Safe - System or component failure shall not propagate sequencially; i.e., design shall fail safe.

E. Design Margins - All space station systems shall be designed to positive margins of safety. Conservative factors of safety shall be provided where critical, single point failure modes of operation cannot be eliminated.

F. All critical life limited components and subsystems shall be designed to allow ground and orbit inspection.

G. Space station configuration design and arrangements shall provide access for inspection of critical hardware, including pyrotechnics (on the ground) after device installation.

H. All components associated with enabling the crew to recognize, isolate, and correct critical subsystem malfunctions for a given space station module must be located onboard and be functionally independent of ground support and external interfaces.

I. Onboard equipment will be provided for checkout, monitoring, warning, and fault isolation to a level consistent with safety and with the in-orbit maintenance and repair approach selected. Emergency control and repair approach selected. Emergency control and repair of failures or damage will also be provided.

J. Primary pressure structural materials shall be non-flammable. Interior walls and secondary structure shall be self-extinguishing.

K. All continuous nonmetallic materials shall be self-extinguishing in the most severe oxidizing environment to which they will be exposed. Means shall be provided for fireproof storage of medical supplies, maintenance supplies, food, tissue, clothing, trash, and for other non-self-extinguishing items, when they are not in use.

L. Materials used in the habitable areas shall not outgas toxic constituents in the lowest pressure environment to which they will be exposed.

M. Potentially explosive containers such as high pressure vessels or volatile gas storage container shall be placed outside of and as remotely as possible from personnel living quarters. The containers shall be isolated and protected so that failure of one will not propagate to others.

N. Redundant equipment, lines, cables, and utility runs which are critical for safety of personnel or mission continuation shall either be located and routed in separate compartments (i.e., separated by a structural wall) or shall be protected against fire, smoke, contamination, overpressure, and shrapnel.

O. Utilities Distribution

1. Hazardous fluid and gas lines shall be double-walled and vented, and shall be barriered or physically separated from power wires and each other.

2. GH_2 and GO_2 lines shall be barriered or separated from each other.

3. Individual ducting shall be provided in all functional areas for the purpose of maintaining a space station atmosphere which is compatible with the crew comfort requirements. Particular emphasis shall be placed on the location of return air ducts from locations which may contribute unpleasant or toxic constituents (e.g., galley, personal hygiene areas, and experiment work areas).

P. Containers and lines for toxic gases shall be placed outside of or as remotely as possible from personnel living and operating quarters, and whenever possible, isolated and/or protected. Provisions shall be made for the detection, containment (i.e., confining) and control (i.e., restoring to a safe condition) of leaks and other potential hazards arising from such equipment.

Q. Critical on-board subsystems will be designed to minimize risk of loss of modules, injury to crew, or damage to shuttle and other interfacing vehicles.

3.2.2 Operating Subsystems

3.2.2.1 Structural and Mechanical Subsystems

A. The space station core module shall be divided into two (or more) separately pressurizable volumes. Each volume will be capable of being sealed off from the other volume(s) and of holding the maximum atmospheric design pressure without structural failures, while the other volume is evacuated, partially pressurized, or pressurized at the maximum design pressure.

B. Staterooms, laboratories, toilets and other areas with restricted access shall provide two separate entry/egress paths for personnel. The two separate paths shall, where possible, lead to different areas on the deck. Where it is not practical to provide doors or normal access routes, the second entry/egress paths may be provided by knock-out panels for emergency use. These should be capable of being opened from either side.

C. At least two egress paths shall be available from each pressurizable volume for emergency egress of personnel during manned ground operations. One external emergency exit shall be available on each pressure volume. The external emergency exits will open outwards and will be compatible with escape provisions in ground operations.

D. Dual Egress

1. Dual egress capability shall be provided from all modules at all stages of buildup. Provisions may be IVA or EVA.

2. Dual shirtsleeve egress shall be provided after initial manning for all modules which are occupied greater than 2 percent of the crew hours available per month. For modules which are not occupied greater than 2 percent of time, dual egress is required; but IVA or EVA egress is acceptable.

E. An internal airlock will be provided which allows for the transfer of IVA personnel between adjacent separately pressurizable volumes when a pressure differential exists or one volume is contaminated. It shall be capable of accommodating two pressure-suited men with backpacks or with umbilicals. One may be incapacitated. Transfer of the two men shall be possible unaided by other personnel. The airlock shall be capable of pressurized or depressurized operation with either of the two connecting volumes depressurized. Use of the airlock shall not cause a rate of pressure drop of more than 0.5 psi/sec. In the connecting volumes for normal operations higher rates are acceptable for emergencies. Three uses of the airlock (entry and return into an unpressurized volume) shall not cause the atmospheric pressure in the pressurized volume to drop below 62 percent of the normal operating pressure.

F. The capability shall be provided which allows the transfer of EVA personnel from one of the pressurizable volumes to and from space. It shall be capable of accommodating two pressure-suited men with backpacks or with umbilicals. One EVA man may be incapacitated. Transfer of the two men shall be possible unaided by the other personnel. The airlock shall be capable of pressurized or depressurized operation with the connecting volume(s) either pressurized or depressurized. Use of the airlock shall not cause a rate of pressure drop of more than 0.5 psi/sec. In the connecting volumes for normal operations, higher rates are acceptable for emergencies. Three uses of the airlock (exit and return) shall not cause the atmospheric pressure in any pressurized volume to drop below 62 percent of the normal operating pressure.

G. The station module shall be capable of being used as an EVA airlock. Provisions shall be made for pressurizing from inside the common module and from the remainder of the space station. Depressurization shall be possible from inside the station module, the rest of the space station, and from outside of the station module. An EVA hatch of 3 feet minimum diameter shall be provided at the opposite end of the module from the berthing port.

H. The flexports shall be provided with a normally habitable atmosphere at all times except when used as an airlock.

I. The flexports shall be located so that the openings into the common module are at least 10 feet distance from the berthing port hatch of the core module.

J. Modules with planned manned occupancy of more than 15 hours per month shall be provided with dual shirtsleeve entry/egress paths. Modules with planned manned occupancy of less than 15 hours per month shall be provided with dual shirtsleeve entry/egress paths, or with one shirtsleeve and one EVA or IVA path.

K. A refuge area, pressure isolatable, is required at far end of the power module. The far end of the power module should also contain an EVA airlock.

L. Access to EVA and IVA airlock suit station(s) shall be provided for all credible emergency conditions. Airlock chamber(s) shall be provided to permit crew access for EVA/IVA operations.

M. Design provisions shall be incorporated to prevent uncontrolled hatch opening due to pressure differential.

N. All walls, bulkheads, hatches, and seals whose integrity is required to maintain pressurization shall be readily accessible for inspection and repair by crewmen in pressurized suits.

O. EVA/IVA Provisions

1. EVA/IVA airlocks shall be located to permit EVA and IVA crew access to and from each pressure isolatable volume. There shall be at least one IVA airlock and this will allow IVA into each pressure isolatable volume. There shall be at least one EVA airlock accessible from either pressure isolatable volume independent of any one EVA airlock. Airlocks in this context can be defined as a specially designed intermediate chamber, individual module, pressure volume, or variation thereof which can satisfy the IVA/EVA function requirements.

2. The capability for rapid depressurization and repressurization of the EVA/IVA airlocks is required. Depressurization control shall be possible from inside and outside the space station as well as from inside the airlock. Repressurization control shall be possible from both inside the space station and inside the airlock.

3. All IVA hatches shall be capable of operation from either side of the hatch, and a capability for equalization of pressure across the hatch shall be provided.

4. Opening of hatches used for EVA must be possible from both inside and outside the space station.

P. Berthing/Docking Port Requirements

1. Provide a backup berthing port on the station at each stage of buildup which allows shuttle berthing and a continuation of buildup.

2. Provide capability to maintain ports and mechanisms on station modules in orbit.

3. Provide one more berthing port on each pressure isolatable volume of the core module than is required for normal build-up, capable of berthing any planned common module. Provide an emergency pressure-tight cover for damaged, leaking core module docking ports.

4. Provide capability to maintain berthing ports and mechanisms on core module in orbit.

5. Provide backup means for release of berthing ports.

6. The capability shall be provided for the separation of unmanned docked vehicles from space station in the event of an uncontrollable emergency on the vehicle which poses a hazard to the space station.

7. Provisions shall be made for the emergency sealing of docking ports in the event of unplanned leakage.

8. Two independent means shall be provided at each docking port for permitting personnel transfer.

9. Design provisions shall be maintained within the docking subsystem which will ensure the ability to dock and perform the initial manning operation using the safety criteria for credible combinations of accidents and/or component malfunctions.

10. Docking shall be possible without utilizing shuttle manipulators.

11. Contingency operational procedures and capability shall be established for on-board repair of the docking utility interface malfunctions and/or redock at an alternate port pending completion of transfer of critical space station consumables from the cargo module.

12. Docking port hatches shall be operable from either side.

Q. Berthing ports shall provide utility interfaces within the pressurized volume. The criteria for the utility interfaces is as follows:

1. Hazardous fluid and gas lines shall be barriered or physically separated from power wires and each other (GO_2 lines shall be considered hazardous in interface areas).

2. GH_2 and GO_2 lines shall be barriered or separated by a minimum of 45 degrees.

3. Redundant fluid and gas lines shall be separated by a minimum of 45 degrees.

4. As a goal, redundant connectors shall be separated a minimum of 45 degrees (a credible accident to, or a credible failure of an interface function or adjacent funciton shall not cause the loss of the redundantly provided function due to proximity of connectors).

5. Connectors that contain signal wires shall be separated from connectors that contain power wires by a minimum of 90 degrees.

R. All berthing ports will be provided with environmental shield covers with the exception of the following:

- Power module +X port
- Core module +X and -X ports and +Z and -Z ports
- Station module -X ports

All covers shall be capable of being opened and closed from within the space station and by EVA.

S. Provide multiple "grab" locations for the shuttle manipulator on each module during each stage of buildup and operations.

T. Structures shall provide facilities for containment of all materials requiring return via the logistics vehicle to prevent contamination of the environment and reduce the hazard of potential fire and toxic conditions.

U. Provisions shall be made for the protection and survival of the full complement of personnel at an emergency level during solar storm activity consistent with the radiation allowables (Table 3.2.2.7-1) and with the specified radiation environment model and duration for solar storms in the orbits.

V. Environmental Shield Requirements

1. Environmental shield shall provide protection for a probability of 0.9 of no micrometeroid penetration of space station modules for ten years.

2. Structures shall provide shielding to limit the crew radiation dosage to limits specified.

3.2.2.2 Environmental Control/Life Support Subsystem

A. Environmental Control Life Support Subsystem - The subsystem maintains emergency reactant storage for the electrical power and reaction control subsystems. In addition, special life support capabilities are provided for emergency conditions.

B. Provisions shall be made for detecting, containing (i.e., confining) and controlling (i.e., restoring to a safe condition) emergencies such as fires, toxic contamination, and depressurization (Table 3.2.2.2-1.

Table 3.2.2.2-1. Emergency Detection

Assembly/Subassembly	Quantity/Location						
	SM 1	SM 2	SM 3	SM 4	Core	Power	Cargo
Special Life Support							
Fire control							
Fire extinguisher pkg	2	2	2	2	1		
Fire detector	1	1	1	1	1		
Explosion detector	1	1	1	1	1	1	1
IVA support							
IVA connects					2		
EVA/PLSS support							
(O_2, H_2O)							X
LiOH canisters		1	1				
Emergency CO_2 removal							
LiOH assembly		1	1				
LiOH storage		1	1				

C. A separate O_2 storage supply shall be provided for emergency use and for supply portable life support equipment.

EPS emergency supply (O_2/H_2) - 164 lb O_2, 20.6 lb H_2

Repressurization (O_2/N_2) - One emergency repressurization of one-half the core module plus two station modules to a pressure of 10.0 psia. The pressure shall be allowed to equalize, then build up gradually to 14.7 psia from normal atmospheric supplies (11,200 cubic feet).

Oxygen system cleanliness requirements shall be established for the manufacture, installation or maintenance operations. In addition, only materials which are compatible with 100 percent O_2 shall be used.

D. While a station module is in the shuttle bay during ground operations and during ascent to orbit, the ability to detect a hazardous atmosphere (Table 3.2.2.2-2) and to provide correction action must be provided prior to suited entry.

E. The cargo module system shall provide alarms and displays to alert the crew to the presence of a dangerous or potentially dangerous situation. The nature of the displays and information to be displayed are TBD.

F. The capability shall be provided to equalize the pressure between space station and the cargo module prior to opening the cargo module hatch.

G. A 96-hour margin of consumables, as a minimum, shall be maintained onboard within each pressure isolatable volume.

H. The capability shall be provided to verify the safe environment and the safe operational status of activated subsystems within the orbiting vehicle (any module) prior to personnel entry initially, and prior to reentry following temporary evacuation.

I. The atmospheric circulation in each volume shall be confined, for normal operations, to that volume, so as to prevent the rapid transfer of airborne contaminants in an emergency to other volumes.

J. The internal and external airlocks shall be capable of repressurization from a vacuum condition with a breathable atmosphere within 30 seconds of being sealed, with an adjacent volume unpressurized.

K. Contaminant control - The MSS atmosphere trace contaminants shall be monitored and controlled to 0.1 of the threshold limit value per constituent. Trace contaminants which may be encountered and their maximal acceptable concentration for continuous exposure shall be as specified in documentation of threshold limit values. (See revised edition, American Conference of Governmental Industrial Hygienists.) Process flow rates contaminant removal subassembly shall be sized by the following contaminants:

Charcoal	- Monomethyl hydrazine
Catalytic oxidizer	- Formaldehyde
Ammonia sorbent	- Ammonia
Acid gas sorbent	- Hydrogen fluoride

The concentration of bacteria in the atmosphere within the pressurized compartments containing crew quarters, process laboratories, or experimental facilities shall be monitored and controlled. RAM is not included.

Table 3.2.2.2-2. Safety Monitoring Requirements for Shuttle Interfaces - Ascent

	Power	Core 1	SM 1	SM 2	SM 3	SM 4	Core 2	SM 5	SM 6
Ascent Measurement									
H_2 tank leak detector	3	4	0	2	2	0	2	0	0
Fire detector	2	2	2	2	2	2	2	2	2
Total	5	6	2	4	4	2	4	2	2
Ascent Control									
H_2 tank vent control	3	4	0	2	2	0	2	0	0
Module vent control	1	1	1	1	1	1	1	1	1
Fan control	1	1	1	1	1	1	1	1	1
Total	5	6	2	4	4	2	4	2	2
PRIOR TO MANNED ENTRY									
On-Orbit Measurement									
Contaminant detector	1	1	1	1	1	1	1	1	1
Module pressure sensor	1	1	1	1	1	1	1	1	1
Air temperature sensor	1	1	1	1	1	1	1	1	1
Total	3	3	3	3	3	3	3	3	3

The atmosphere constituents, including harmful airborne trace contaminants and odors will be monitored and controlled in each separate pressure isolatable volume.

L. The capability shall be provided for providing a habitable shirtsleeve atmosphere, humidity control, temperature control, fluid and food supplies, hygiene and waste management requirements, for the whole crew for a minimum period of 96 hours:

1. With any one pressurizable volume deactivated, isolated and vacated due to an accident

2. With any credible combination of a subsystem deactivated as a result of an accident and a portion of a redundant or backup subsystem inactive for maintenance.

M. Design and operational provisions within all the ECLSS subassemblies, such as those indicated below for CO_2 malfunction, shall be made which satisfy the safety criteria for credible accident and equipment malfunctions established in the operability portion of the general requirements section of this specification.

N. Atmospheric Storage and Supply

1. Storage bottles, O_2 and N_2 surge tanks, lines and connections shall have as a minimum a design burst pressure factor of safety of 2.00 and a requirement for hydrostatically proof pressure testing of 150 percent of the design operating pressure.

2. High pressure O_2 and N_2 bottles and their installation shall include the following design requirements:

a. Provide a means for preventing shrapnel from causing loss of and/or injury of personnel due to a bottle rupture.

b. Provide a means of preventing or reducing the possible injurious effect of a pressure wave from exploding O_2 or air storage bottle.

c. Provide a means of preventing loss of space station pressure due to damage from an explosive rupture of an O_2 and/or air storage bottle.

O. CO_2 Management

1. Contingency operational procedures and design capability shall be provided to safely handle a CO_2 removal malfunction as follows:

   a. Automatic check of CO_2 level at two-hour intervals

   b. Provide automatic alarm and warning when CO_2 level reaches a distracting discomfort level of 16 mm Hg partial pressure.

   c. Initiate troubleshooting and repair when normal operating CO_2 level increases at a rate indicating a CO_2 removal malfunction.

2. Design capability for monitoring the level of H_2 and CH_4 within the space station due to inadvertent leakage shall be provided together with procedures for troubleshooting and restoring the system to a safe condition prior to the development of combustible mixtures.

3. Design capability shall be provided to utilize the emergency O_2 supply and provide automatic crew caution and warning when a loss of the H_2O electrolysis unit is detected by an excessive drop in O_2 partial pressure.

4. Contingency operational procedures shall be established for troubleshooting and restoring a malfunctioning H_2O electrolysis subassembly in sufficient time to preclude calling for emergency resupply and/or rescue.

P. Atmospheric Control

1. Contingency procedures and a design capability shall be established to sense the excessive flow of GN_2 and shutoff of the source until maintenance can be performed to correct the malfunction.

2. A redundant O_2 partial pressure monitoring system shall be used in each space station volume to control the required flow of O_2 and N_2 gases. Trend data shall be recorded by the information subsystem (ISS) and caution and warning to the crew provided when a critical trend is predicted. Automatic recalibration of the monitoring system will be initiated when the redundant monitoring system shows a difference in excess of TBD psi.

3. Operational procedures and design capability shall be provided which prevent an excessive increase in space station temperature in accordance with the safety requirements specified in the operability portion of the general requirements

section of this specification. An analysis shall be developed which evaluates temperature rise associated with the interrelationship of credible accident and/or component malfunctions and the thermal loading during an emergency operation.

4. Requirements for information subsystem shall be established to automatically monitor and provide trend indications of the critical trace contaminants, giving crew caution and warning when trend predictions appear hazardous to personnel health and/or experiments.

5. Operational procedures to troubleshoot and restore the space station trace contaminate to acceptable levels shall be provided.

6. Criteria and process controls for the elimination and prevention of all toxic materials from entering the space station during design, manufacturing and resupply shall be established.

7. Checklists for each subsystem which indicate the equipment that may be adversely affected by credible contaminates shall be provided and corrective action plans for their reduction or control shall be established.

8. Operational procedures shall be established for periodic replacement of debris filters and contingency replacement when excess dust accumulates in the space station.

Q. Active Thermal Control

1. Operational procedures to reduce heat generated by electrical equipment on a priority basis shall be developed (that is, establish a method of sequential shutdown of nonessential electrical equipment when space station temperature increase indicates a possible malfunction of the active thermal control subsystem). A method of troubleshooting isolating and restoring of the subsystem within a safe time span shall be provided including the requirement for an emergency resupply or rescue within 96 hours of potentially catastrophic effect.

2. The installation of fluorocarbon (F/C) coolant loop plumbing and connectors which are located within the space station volumes shall be placed in separate leak-tight containers which have automatic leak detectors, and ISS caution and warning indication of leakage provided. A procedure for troubleshooting, isolating and repair of the malfunction shall also be developed.

3. Design and operational procedure for monitoring the space station water coolant loop and F/C coolant loop for leakage in either direction shall be provided together with provision for the isolation and replacement of the suspected intercooler malfunctioning unit.

R. Water Management

1. Operational procedures and capabilities for restoration of the potable water reclamation unit while the emergency H_2O supply is being used shall be established including a requirement for resupply and/or rescue when two days of emergency H_2O remains and repair has not been achieved as well as provisions for rationing of the remaining potable water to the crew.

2. Design requirements for the use of redundant contamination detectors within the potable water supply shall be established which will provide automatic warning of an increase in a dangerous contaminate. Operational procedures for troubleshooting and restoring of the subsystem prior to a need for an emergency and for resupply shall also be developed.

S. Food Management

1. Capability to monitor food preparation ovens for possible radiation leakage shall be provided including caution and warning to crew members in the vicinity of the oven.

3.2.2.3 Electrical Power Subsystem

A. Electrical Power Subsystem - The electrical power subsystem shall store, generate, regulate, control, and condition electrical power for backup and emergency contingencies (except for emergency fuel cell reactants which are stored by the ECLSS).

B. Provide electrical power (at the load buses) capable of sustaining the following loads (watts).

Table 3.2.2.3-1. Emergency Electrical Loads

		14 Hour Day		10 Hour Night	
	24 Hour Average	Orbit Light Period	Orbit Dark Period	Orbit Light Period	Orbit Dark Period
Initial Station Emergency	1,500	1,500	1,500	1,500	1,500

C. Power requirements for recreation/crew care/exercise:

Worst days - emergency power approximately 112.8 watts avg/24 hr
- X-ray
- Sterilizer
- Medical light
- Electrocardiogram

D. During emergency operations lighting will be limited to 40 watts.

E. Cable runs shall be suitably enclosed or otherwise protected to minimize hazards to the crew and provide maximum mechanical protection for the conductors.

F. Bus isolation shall be such that failure of one bus will not cause failure of another bus.

G. The capability shall be provided to supply power to perform emergency operations for a minimum of 96 hours with one pressure volume inactivated, isolated and vacated due to an accident.

H. The capability shall be provided for the detection of time-critical malfunctions of the EPS or overloads on the EPS, and the automatic switching to a safe mode of operation.

I. Design requirements shall be established for the use of non-sparking and/or non-spark propagating electrical equipment and connectors in all areas where combustible mixtures may collect.

J. Electrical equipment used within the space station where condensation may collect as a result of an ECLSS humidity control malfunction shall be designed to function with an environmental condition with 100 percent humidity for a period of 96 hours maximum duration.

K. In the case of a failure of part of the primary power source where the normal load cannot be sustained, the remaining portion of the primary source shall automatically assume the backup load requirements. In case of failure of both the primary and backup power source where the backup load cannot be sustained, the separate emergency power source shall automatically assume the emergency load requirements.

L. EPS together with ISS shall provide the necessary electrical distribution and hardware for control of the EPS from two separate and redundant control centers, one center in each pressure isolatable volume.

M. EPS shall be designed for fail-safe operation and where possible will result in only gradual degradation and loss of function following failures.

N. All circuits shall be provided with circuit protection devices. Circuit protection devices for circuits required for emergency operations will be re-setable from the control centers.

O. The emergency distribution can be the same or integrated within the primary distribution (normal redundant requirements); however, the critical life support functions shall be capable of being electrically isolated from the general distribution through automatic load shedding of noncritical functions.

P. Electrical distribution panels shall be adequately enclosed or otherwise protected to minimize hazards to the crew and provide maximum mechanical protection for the electrical subsystem and components.

3.2.2.4 Guidance and Control Subsystem

A. Loss of pressurization in a volume may be caused by accidental penetration of an outside wall with the maximum dimensions of the hole being two inches. The station shall be able to stabilize for docking/berthing within TBD hours.

B. Operational procedures and/or design provisions for the critical guidance and control functions shall be established which will ensure the ability to dock the shuttle with the station, both during the premanning and manned phases.

C. Contingency operational procedures and crew training shall be provided to allow manual computation of guidance parameters for orbit maintenance of the space station in the event of a computer malfunction.

D. Emergency flight control of space station shall be provided from local manual control device in each pressure volume in core module.

3.2.2.5 Reaction Control Subsystem

A. Safety factor to be applied to pressurized vessels in normally habitable areas shall be at least 4 and in other areas, 2.

B. Provide RCS attitude control for docking capability

Unmanned Operations

0 - Failures, use Set 1 and Set 2

1 - Failure (any engine), use either/or Set 1, Set 2

2 - Failures (Set 1 and 2) any engine

3 - Failures, yaw engine, no yaw

Manned Operations

Same as unmanned operations; after thrustor failure, quad can be replaced. Docking function is not time critical.

C. The RCS shall be capable of operation at each failure level as shown below:

Failures	Requirement Interpretation
0	Provide all functions Size accumulators for 12-hour impulse requirement with no reserve allowance
1	Provide all functions Orbit makeup can be delayed until repair completed If repair time greater than 5 days, utilize EPS and ECLSS capability for orbit makeup
2	Degrade operations CMG desaturation once/orbit Orbit makeup delayed until repair completed Utilize EPS and ECLSS capability as required
3	Provide docking capability Utilize EPS and ECLSS capability as required

D. Tanks used as gas accumulators in inhabited areas shall be designed to a factor of safety of 4.0 as a minimum. Tank supports shall be designed to restrain the tank under propulsive effects of rapidly escaping gas.

3.2.2.6 Information Subsystem

A. Supervisory Programs - These programs shall provide the processing and control necessary to coordinate and schedule the work of the applications programs and carry out service functions for them. The supervisory programs shall handle input/output and the queueing of messages and data. They shall coordinate and optimize machine loads under various conditions and shall service interrupts and deal with errors or emergency conditions.

B. ISS shall provide the following:

Alarm override of paging system
Local monitor alarm - one in each module
Emergency G&C control
On-board checkout - verify emergency capability

C. The capability shall be provided to detect malfunctions in the operations of the subsystems and experiments using data provided by subsystems and experiments, trace the malfunction to the failed inflight replaceable unit, and display the information necessary for corrective action.

D. For those malfunctions and/or hazards which may result in time-critical emergencies, provisions shall be made for the automatic switching to a safe mode of operation, and for caution and warning to personnel.

E. Caution and warning information relating to time-critical emergencies shall be provided by at least two separate means, not using any common hardware.

F. No single failure nor equipment down for maintenance shall prevent the communications of data and information necessary to handle a space station emergency situation.

G. Safety monitor during buildup:

In cargo bay

Hardware measurements for all modules

Quiescent operations - unmanned

Transient subsystem status once daily for 1 sec transmission time

Verify core module safety

Crew ingress

Pressurize adapter
Equalize pressure between shuttle and adapter
Open shuttle/adapter hatch
Correct CM/shuttle interface lines
Verify CM temperature and pressure
Equalize pressure between adapter and CM
Open adapter (CM hatch)
Crew CM ingress (suited)
Verify shuttle/adapter/CM interface
Verify CM integrity
Verify station safety

H. The capability shall be provided to monitor the status of EVA personnel by two independent means. These data shall be available at the control centers.

I. The capability shall be provided to determine the existence of emergencies such as fires, toxic contamination, depressurization, structural damage, etc., using data provided by other subsystems and experiments. Appropriate caution and warning information shall be provided to affected crew members for such situations, informing them of the type and location of the emergency, and of the necessary corrective action (Table 3.2.2.2-1).

J. A backup control center shall be provided in a different pressure volume from the primary control center. It shall have the capability, at the minimum, (1) to provide the command and control functions to operate the active subsystems and experiments in the event of loss of access to the volume containing the primary control center due to an accident, and (2) to provide sufficient monitoring, checkout, command and control functions of the subsystems and experiments in the affected volume to ensure safety, prevent further damage to equipment, and determine repair, IVA maintenance and resupply requirements to restore shirtsleeve access to the affected volume.

K. The space station shall be provided with an override capability to exercise flight control over the shuttle from stationkeeping to hard dock. The SS control centers shall be capable of monitoring and controlling MSS/shuttle closing ranges, rates, and attitudes to ensure structural integrity and crew safety during terminal rendezvous and docking operations.

3.2.2.7 Crew and Habitability Subsystem

A. Crew Habitability Subsystem - The subsystem provides emergency oxygen masks and radiation monitoring devices for the crew.

B. The atmosphere constituents, including harmful airborne trace contaminants shall be monitored and controlled in each pressurized compartment of the space station.

C. In the event of space station pressure hull damage resulting in pressure decay in a pressure volume, the duration of acceptable crew performance shall be considered to be that period of time until a partial pressure of oxygen of 1.9 psi is reached.

D. O_2 emergency flow (22 lb/man-hr for 30 minutes) shall be required for IVA support.

E. Microbiologically and bacteriologically contaminated waste material shall be disinfected as close as possible to its source prior to storage, processing or disposal; e.g., small animal waste and other bioscience particulate matter.

F. Special protective garments and equipment shall be provided for personnel working in a toxic environment or near potentially toxic station elements.

G. Deployment and initiation of operations considered hazardous shall be checked out from a safe location before exposing crewmen to the potential hazards.

H. Emergency personnel equipment shall be provided and located in each module and shall consist of:

1. Three emergency oxygen full-face masks with integral portable oxygen bottles of five-minute capacity

2. Two liquid-cooled garments (LCG), pressure garment assemblies (PGA), and portable life support systems (PLSS)

3. IVA umbilical connections and hoses sufficient to reach all interior volumes for repair

I. Personal radiation dosimeters shall be provided for each crewman. They shall be worn at all times (in pockets on crew garments), and shall be capable of measuring accumulated radiation dosage.

J. Emergency general crew equipment shall consist of portable lights and a medical accessories (first aid) kit. They shall satisfy the following performance requirements.

1. Total of one portable light per module shall be provided for emergency maintenance or inspection in the event of power failure. Each portable light shall be capable of providing floodlight-type direct illumination of 100 foot candles at a distance of 10 feet, and not less than 50 foot candles at this same distance after three hours of continuous operation. Each portable light shall have a carrying handle and actuation device compatible for use with a gloved hand (suited/pressurized operations). Capability to recharge portable light batteries shall be provided.

2. Medical accessories kit - A medical accessories (first aid) kit shall be provided in each module except in the module containing the medical treatment area. This kit shall be capable of providing for medical emergencies. This kit shall include such items as oral drugs, injectable drugs, dressings, bandages, and topical agents.

K. In addition to the personal radiation dosimeters provided as personal equipment and worn by the crewmen, suitable devices shall be provided at selected locations within each module to measure ambient radiation levels as well as cumulative radiation dosage.

L. Emergency biomedical equipment will be provided and located in each habitable module and will be readily accessible to the crew.

M. The following equipment shall be provided for medical and dental care of the crew:

Lower body negative pressure devices
Mass measurement device
Mobile X-ray unit
Examination tables (details - to be determined)
Surgical instruments (details - to be determined)
Sterilizer
Stowage cabinets
Miscellaneous portable diagnostic equipment (details - TBD)

N. Food Management - A backup galley shall provide food service in the event of loss of the primary galley for six men up to 30 days. The backup galley shall contain, as a minimum:

Dried food
Reconstitution unit
Thermodried food
Skylab heating trays

O. Provisions shall be made for emergency medical treatment of sick or injured personnel for a minimum period of 96 hours. All potential conditions and injuries consistent with the age, physical and mental condition, and planned stay time of the on-board personnel shall be considered.

P. Provisions shall be made for the restraint of irrational personnel.

Q. Provisions for suited IVA, EVA, and entry into hazardous areas shall be based on the operation being conducted by at least two men. Provisions shall be made for the rescue of one man by the other in an emergency.

R. Provisions shall be made for emergency treatment of injured personnel following an accident which renders the pressurizable volume containing the primary medical facilities unavailable.

S. Pressure suits, backpacks and umbilicals, and related support equipment shall be provided in readily available locations so that two suits may be reached and donned from any location in the space station, with any one pressurizable volume inaccessible due to an accident.

T. Emergency suits required in the space station core module shall be in readily accessible locations within each pressure isolatable volume.

U. The capability shall be provided on the space station for the detection of malfunctions and/or hazards, tracing to the failed replaceable unit, and the display of information to the crew necessary for corrective action.

V. The cargo module system shall provide emergency lighting to support crew activities.

W. Provisions shall be made for the protection and survival of the whole crew during solar storm activities as defined by the design mission radiation model. The radiation dosage limitations defined in Table 3.2.2.7-1 shall apply.

X. Irradiation diagnostic devices will be shielded such that radiation protection is afforded the operator and inflight personnel other than the patient. Shielding shall be of such design that flight crew in the vicinity of operating irradiation devices will not accumulate a radiation dose, including the natural radiation, great enough to exceed the radiation limits in Table 3.2.2.7-1.

Table 3.2.2.7-1. Allowable Radiation Limits

Organ	Limit Dose (REM)					
	Depth	Daily*	30-Day	Quarterly**	Yearly	Career
Skin	(0.1 mm)	0.6	75	105	225	1200
Eye	(3.0 mm)	0.3	37	52	112	600
Marrow	(5.0 mm)	0.2	25	35	75	400

* One year average

** May be allowed for two consecutive quarters with six months restriction from further exposure to maintain yearly limit

3.2.3 Shuttle Interfaces

A. The space shuttle shall be capable of supporting an on-call emergency capability of MSS rendezvous and berthing within 48 hours after notification.

B. Provide backup means for returning module to shuttle cargo bay in the event of shuttle manipulator failure.

C. Provide backup release on shuttle manipulator.

D. Provide independent emergency means for folding manipulator out of way following failure.

4.0 TRADE STUDIES

System safety considerations were strong drivers for trade studies and special studies performed for the MSS. Candidate functions, operations and configurations were reviewed for compliance with the safety ground rules, constraints, and criteria. Hazards were identified and alternatives were evaluated for mission performance including all feasible safety features and a qualitative comparison of residual hazards. The selected configuration was reviewed for hazard elimination according to the hazard reduction precedence sequence. These special studies resulted in some new requirements which are listed in Section 3.0 of this report and in the Preliminary Performance Specification, DRL 66.

While all safety criteria proved to be influential in design selection, several selected criteria had a notable effect on the assembled MSS configuration. The requirement for multiple, isolatable volumes drove the distribution of subsystem and emergency capabilities. Where a critical function is lost, crew survival provisions must be available for 96 hours to permit rescue by the shuttle. The program requirement for response is 48 hours, which leaves 48 hours for shuttle or station contingency. Adequate subsystem redundancy must be distributed throughout the isolatable volumes to meet critical function failure tolerance criteria. The requirement for two entry/egress paths drove the internal module configuration to a longitudinal floor with separate paths on either side and to flexports between habitable modules. Flexports are fixed tunnels connecting station modules (in addition to the normal path through the core module) and providing emergency, shirtsleeve passage. Hazard detection means were required for every alternative.

A summary of safety considerations applied to configuration and operations trades is contained in Table 4.0-1.

Special safety studies have run the gamut from functional considerations at the system level to the amount of subsystem redundancy required for emergency back-up.

The special studies summarized in this section are only a portion of those performed but represent the most significant for the MSS. Studies at the system level are included that produced an MSS design that was safe to operate, for example:

1. Multiple volumes with capability to maintain life support and (reduced) station operation following loss of any given volume (or module).

2. More than one shirtsleeve escape route from any normally inhabited module to another habitable module (actually to the remainder of the station.) Normal egress through end hatch into core module -- alternate egress through flexport to adjacent station module.

Table 4.0-1. Safety Considerations for Trade Alternatives

Trade	Alternatives	Safety Considerations
A. System Sizing	1. Minimize conversion from 6-man to 12-man. 2. Optimize at 6-man level. 3. Provide capability for less than 6-man and more than 6-man level.	Provide critical functions and adequate crew survival capability at each stage of manned operation. Survival capability must be provided in each isolatable volume.
B. Cargo Operations	1. Up/down same launch. 2. Up/stay with fluid transfer. 3. Up/stay without fluid transfer.	Transfer of high pressure, high energy fluid containers involves hazards of collision with impact damage and possible rupture. It would also introduce hazardous equipment into inhabited modules. Transfer of high pressure gas to station modules would involve disconnects, and high pressure lines and containers in the station modules. Container pressures in the cargo module would have to be even higher to permit transfer to the station with a weight and hazard penalty on the cargo module. Concept 2 permits retention of high pressure storage vessels in the cargo module with pressure reduction to the disconnects and station modules *thus reducing crew exposure markedly.*
C. Dual Shirtsleeve Egress	1. Station modules only. 2. Station modules plus special modules. 3. All modules including RAM's.	The core and station modules are constantly on-orbit and normally inhabited by the crew. Dual shirtsleeve egress between pressure isolatable volumes insures egress to a safe volume in any emergency. While the power boom is an integral part of the MSS it is rarely inhabited by the crew and special precautions can be taken when occupied.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
C. Dual Shirtsleeve Egress (Continued)		The RAM's and cargo modules are attached to the station temporarily and connecting and disconnecting flexports would increase crew tasks significantly. Also, crew occupancy is low so that special precautions can be taken when occupied. Alternate means of egress by means of EVA is still possible.
D. Module Diameter	1. 15 ft. 2. 14 ft.	The 14 ft diameter provides less (but adequate) volume for safety features, and more clearance in shuttle cargo bay for safe transport.
	3. Less than 14 ft.	Usable volume for the small diameters decreases rapidly, thereby limiting safety features.
E. Subsystem Assemblies	1. Devoted modules (EPS, ECLSS, RCS). 2. Dual purpose module, (EPS/ECLSS/RCS). 3. Distributed subsystems.	Subsystems cannot be safety centralized because each isolatable volume must contain emergency capability for the entire crew; e.g., the entire power supply could be placed in a dedicated module, but sufficient power must be available in each volume to sustain life for at least 96 hours. Concept 2 with redundancy in the two pressure isolatable volumes best meets safety criteria.
F. Y-Plane Modules	1. None. 2. Cargo only. 3. Station modules (common or special). 4. RAM's. 5. Cargo plus RAM's.	Y-plane modules must also meet all the safety criteria. Safety must monitor each arrangement for criteria compliance. No significant safety issues.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
G. Pressure Volumes	1. Two independent. 2. Three with two out of three required. 3. Four with two out of four required.	Alternate passages for rapid egress is required between pressure volumes for safety. Backup EVA/IVA access to each pressure volume is also required. Loss of a volume which could separate the crew into isolated volumes is highly undesirable and reduces safety. The station must maintain a capability to repressurize a volume that has been depressurized.
H. RAM Accomodations (initial Station).	1. Two attached (both earth oriented). 2. Two attached (earth and zenith oriented). 3. Two attached plus one service port. 4. Accommodate two (attached or detached).	Each attached RAM must be monitored for hazardous conditions. Location is not a safety problem. When the RAM is inhabited for an appreciable time period, dual access/egress routes are required. Special experimental materials may require special handling.
I. RAM Sizing	1. Same as Phase B. 2. Same as common modules.	RAM size may influence the safety precautions to be imposed.
J. Crew Quarters	1. Six in a single volume. 2. Split between modules.	As long as dual egress paths are required and emergency provisions are located in all isolatable volumes, the safety criteria are satisfied.
K. ECLSS Assembly Sizing	1. Six-man units initial and growth.	See Item J.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
K. ECLSS Assembly Sizing (Continued)	2. Six-man initial and twelve-man in the growth version. 3. Less than six-man units.	
L. Floor Orientation (Secondary Structure)	1. Transverse 2. Longitudinal. 3. Both.	Longitudinal is easier to make safe because of the dual egress path criterion. Transverse is easier to compartment for containing hazards. A judicious combination of both would provide multiple egress paths as well as hazard isolation; i.e., a single longitudinal floor with compartments around special functions.
M. Internal Arrangements (if Longitudinal)	1. Single level. 2. Split level.	Split level is much safer when access paths are available around each end of the floor. See Item L.
N. Berthing Ports per Module	1. Single end all station modules. 2. Dual ends all station modules. 3. Dual ends on selected modules.	"Dual ends" (in addition to the flexport) increases the safety of enclosed crew by 1) increasing number of exits and 2) increasing rescue flexibility. Shuttle berthing could occur at the outer end of any station module for crew off-loading. Crew EVA could be accomplished from the open end by utilizing the module as an airlock.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
O. Experiment Airlock Location	1. Internal to general purpose laboratory. 2. External single location. 3. External and movable.	Laboratory hazards should not be allowed to block the airlock. The most flexibility is obtained by making the airlock movable, but the moving would be a hazardous operation involving the shuttle.
P. RCS Engine Fuel Location	1. In cargo module(s). 2. On space station. 3. Split (station and cargo).	Single cargo module storage would not provide an emergency supply. Multiple cargo modules may not be at the MSS at the same time. Several locations on the station would provide the necessary redundancy (e.g., power boom and core module) but the amount in the core module must be limited to reduce the leak/explosion hazard to the crew. Leaving the major amount of fuel in the cargo module(s) and providing multiple MSS locations for partial storage is the safest.
Q. High Gain Antenna Location	1. On station special modules. 2. On station common modules. 3. External movable.	Retention of back-up, omni antennas on each isolatable volume would fulfill the emergency communication criterion.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
R. Solar Array Location	1. Power boom single end. 2. Power boom dual ends. 3. Integrated with end mounted modules.	A single end location requires a back-up power source for emergency. Dual ends may provide the back-up redundancy but complicate shuttle berthing.
S. Initial Build-Up Sequence	1. Core module up first. Power module up next. 2. Power module up first. Core module up next.	No significant safety issues.
T. Core Modules	1. Single initial and growth. 2. Single initial and growth to dual. 3. Dual initial and growth. 4. None.	Core module must support dual volume concept at all stages of manned operation.
U. Manipulator	1. Shuttle only. 2. Shuttle and station.	Failure of a single shuttle manipulator would prevent completion of the module installation, and may lose the module. Even though the manipulator internal mechanism were redundant, further back-up is safer; i.e., place manipulators on both shuttle and station.

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
V. EVA/IVA Airlocks	1. Two airlocks with both EVA and IVA capability. 2. One airlock with dual capability, one airlock with EVA capability, and one airlock with IVA capability. 3. Two airlocks with EVA capability and two airlocks with IVA capability.	Any of these alternatives provides a back-up for emergency. The four airlock alternative is the safest because four failures are necessary to prevent any suited transfer between pressurized and unpressurized modules.
W. Berthing Port Commonality	1. All common. 2. Separate for power. 3. Unique.	Each type of berthing port must conform to safety criteria. The safety advantage for common ports is redundancy during build-up, i.e, for the condition of one station module already berthed and one unable to berth, the opposite side of the core module could be used temporarily for both station modules. This allows the use of a flexport.
X. Flexport Options	1. Normally open. 2. Normally closed.	Flexports are used only in an emergency. The transmission of dangerous products of the emergency should be kept to a minimum. The safest is to keep the flexport hatches closed.
Y. Aisle/Passageway	1. Center 2. Side 3. Subfloor access.	

Table 4.0-1. Safety Considerations for Trade Alternatives (Cont)

Trade	Alternatives	Safety Considerations
Z. Module Spacing	1. Six inches. 2. Twelve inches. 3. Twenty-four inches. 4. Forty-eight inches.	Six and twelve inches are clearly too close for EVA repair capability. Twenty-four inches begins to be more open, but forty-eight is definitely the safest of all. The larger spacing also allows for berthing port misalignment.

3. Dual IVA paths available/Dual EVA paths available.

4. Consistent failure and accident tolerance criteria applied to all subsystems supplying critical functions; e.g., fail operate, fail reduced, fail safe until rescue.

5. High energy pressure vessels located outside of normally inhabited modules or pressure vessels/accumulators inhabited modules designed to >4.0 safety factor.

6. Double containment of all hazardous fluids (tanks, lines and fittings).

7. Restraint/pressure equalizing requirement for all hatches with Δ P.

Additional safety analyses are presented which illustrate the depth of detail required to support the system choices.

4.1 MULTIPLE VOLUMES

If an accident occurs which could result in depressurization, atmospheric contamination, or loss of some critical function, the crew must be able to survive safely in a separate pressurized area until the affected volume is restored to a habitable condition or until they are rescued by a shuttle. As many as 48 to 96 hours may be required to reach the station and this set the minimum time for crew survival onboard the station. These considerations led to the first of the system safety criteria in Table 4.0-1 which required the station to be divided into separate pressure-isolatable volumes.

The design solution consists of arranging the habitable modules into pressure-isolatable volumes of approximately equal capabilities, as shown in Figure 4.1-1. Each of the two volumes includes half of the core module, two station modules with crew support provisions, and provisions for attaching cargo modules and research application modules (RAM's). Each of the two volumes contains complete environmental control, thermal control and information subsystems, a control center, docking/berthing capability, and emergency supplies. Each volume can support the crew of six indefinitely (subject to adequate consumables) independently of the other volume. Primary electrical power is supplied to both volumes from a common power module and is available to both volumes even if one has been evacuated.

One of the more credible reasons for evacuating one volume is that the atmosphere has become contaminated, possibly with smoke from a fire. The air circulation systems in the two volumes are, therefore, kept separate so that contaminants from one volume will not be introduced into the other volume. It was possible to design the station so that only the affected module could be isolated following an accident. However, this would require, for example, that each environmental control subsystem be able to supply other modules in the volume, and that many of the air ducts would have to be capable of operating in a vacuum (in the event of depressurization of that area). The

valving system would also be considerably more complex. Because of these reasons, the simpler approach with each environmental control subsystem servicing its own volume was adopted. This design allowed for individual module isolation in many emergency situations. Loss of atmospheric and thermal control, however, would allow for only limited shirtsleeve operations in that volume.

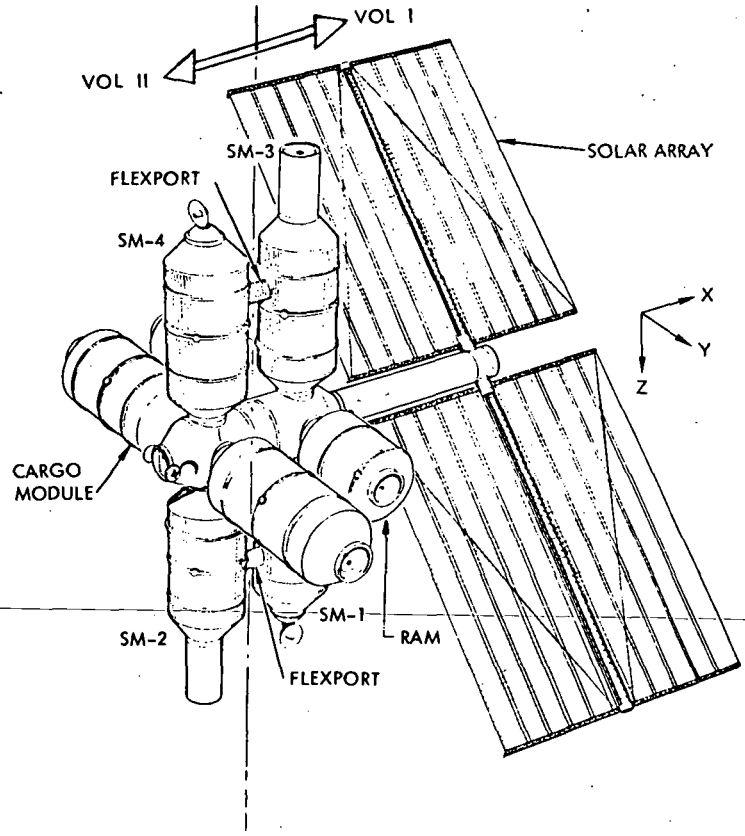

Figure 4.1-1. Modular Space Station - Dual Volumes

4.2 DUAL SHIRTSLEEVE EGRESS

Because of the key influence of the system safety criterion for dual entry and egress on the configurational arrangement of the space station and of each module, a special evaluation was made of the criterion and of the means for implementing it.

System safety goals require that no credible combination of malfunctions and accidents result in serious injury to personnel or to crew abandonment of the station. Of the 17 credible accidents defined, three produce a situation which may require evacuation of a module, and at the same time may preclude

access to any one exit. These credible accidents are fire, explosion, and accident in a hatch (i.e., opening between modules). For example, flames, fumes, or heat from fire close to an opening may prevent personnel from exiting from the affected module, and the men may suffocate if another exit route were not available to an area with an independently controlled atmosphere. Similarly, an explosion could result in a fire near an opening, and an accident in an opening may injure or otherwise endanger personnel but prevent their exit or rescue by other personnel.

To satisfy the system safety goal, it was necessary to provide for two or more ways in and out of each area, located and separated from each other so that a single accident would not prevent access to both of them. This therefore led to the criterion for two or more entry/egress paths (see Table 4.0-1).

The separation of the two paths by airtight partitions allowed a crewman to get past a fire or a source of fumes to gain access to an exit: if a module were divided by a floor, as shown in Figure 4.2-1, and a fire started in Area C, a man stationed at A can still get past the fire to get to the exit B by going below the floow, as shown by the dotted line, without having to pass through the fire or fumes. The 10-foot separation is determined by the judgment that the immediately dangerous area (heat, flames, debris) in a credible accident would extend over a distance of about 5 feet. Two paths in the same open area separated by at least 10 feet should therefore provide at least one safe path past the accident area.

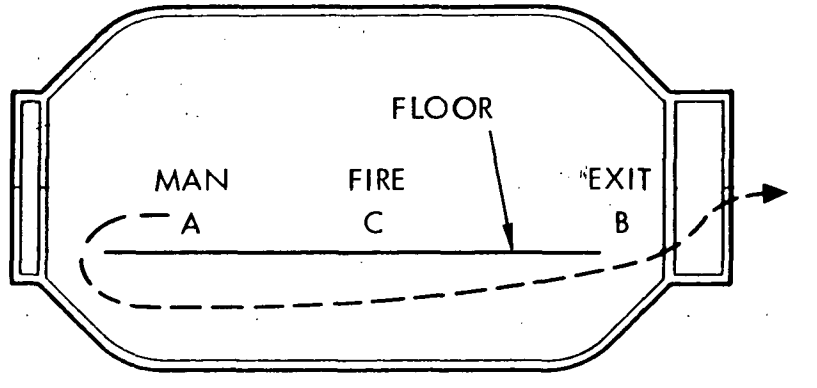

Figure 4.2-1. Dual Egress Path Provided by Floor in Module

Three alternative barbell/cruciform configuration solutions were considered for applying this criterion to the space station configuration (Figure 4.2-2). They are open configurations, in which all modules were attached at one end only to a common core module, but using 1) auxiliary emergency secondary passages between modules, called flexports, to connect adjacent manned modules at the other end; 2) an emergency volume attached at

the far end, internally to the module, into which the crew could take refuge until rescue by the shuttle or until the safe environment was restored in the affected module; and 3) an emergency volume attached externally at the far end to the module.

Table 4.2-1 summarizes the evaluation of these alternatives. Additional design complexity and weight results from each of the three solutions. The flexport solution required development of the mechanisms and materials to deploy, dock, and take up some deflections. The emergency volume concepts required an additional environmental control/life support subsystem (ECLSS) in each emergency volume which was separate from the ECLSS of the module to which it was attached, so that it would not be contaminated by fumes from the affected module.

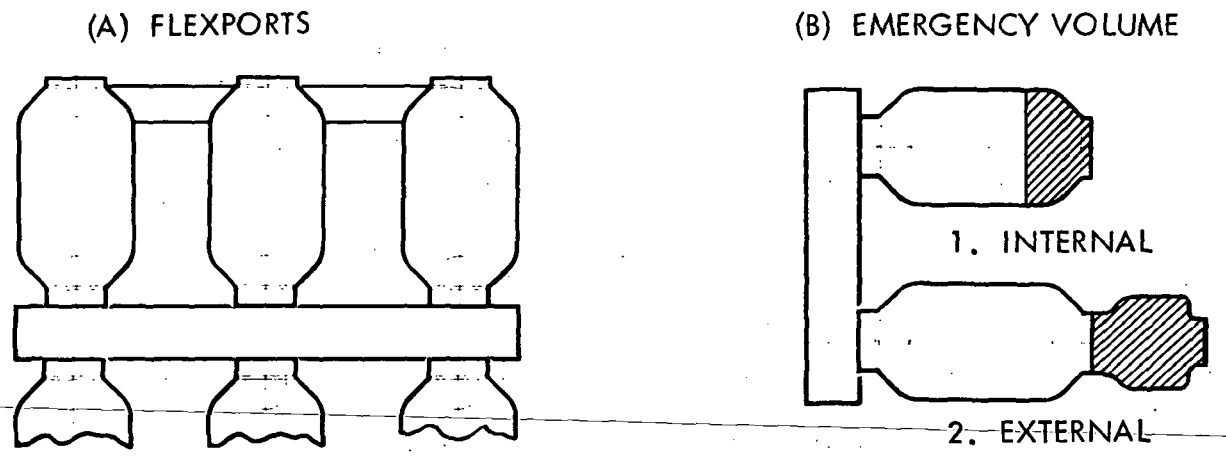

Figure 4.2-2. Alternative Solutions for Dual Egress

The selected solution was the use of flexports between adjacent station modules in the preferred configuration. Special safety provisions would be applied to cargo modules and RAM's, which have a low crew occupancy rate. Such provisions may consist of special procedures to check the status of potentially hazardous equipment before entry into the modules (as opposed to routine entry without special safety checks); special fire prevention, detection, and suppression means; the avoidance of potentially hazardous equipment near the exit. Similar special safety provisions should be applied during buildup of the station when one or more manned modules do not have an adjacent module for connection by a flexport.

The flexports consist, functionally, of a tubular connection between two adjacent modules which are capable of allowing rapid shirtsleeve transfer of personnel between the modules. They are of a diameter (3 feet or more) to allow IVA suited men to return to a depressurized or contaminated module for maintenance and repair. The flexports are stowed during launch of the

Table 4.2-1. Evaluation of Alternative Solutions for Dual Egress

Flexports (Secondary Passages)	1. Operational restrictions in buildup
	2. Increased leakage
	3. Additional mechanical devices
Emergency Volume - Internal	1. Added ECLSS
	2. Additional pressure bulkhead and structure
	3. Loss of useful volume
Emergency Volume - External	1. Added ECLSS
	2. Additional mechanical device

modules within the module moldline and are deployed and joined to the adjacent module after hard docking of the two modules to the core module. They can be disconnected and retracted for returning modules to earth. While connected, the flexports must have sufficient flexibility to accept normal relative motions of the connected modules due to structural flexibility, and manufacturing and assembly tolerances, Figures 4.2-2 and 4.2-3.

The purpose of the flexports is to provide an emergency exit from a module into another module in the event of an emergency which either (a) prevents exit through the normal berthing port hatch into the core module, or (b) makes it safer to exit through the flexport.

Functional requirements for the flexport hatches to achieve this are:

a) Reasonably rapid opening of hatches (if closed).

b) Shirtsleeve atmosphere in flexport at all times spacecraft is manned and flexport operational.

c) Reasonably rapid shutting of hatches. This is desirable for hatches between modules in one volume, but is a <u>requirement</u> between volumes (see "d").

d) <u>All</u> hatches between volumes to be shut, and confirmed to be shut, after evacuation of a volume, with minimum crew actions.

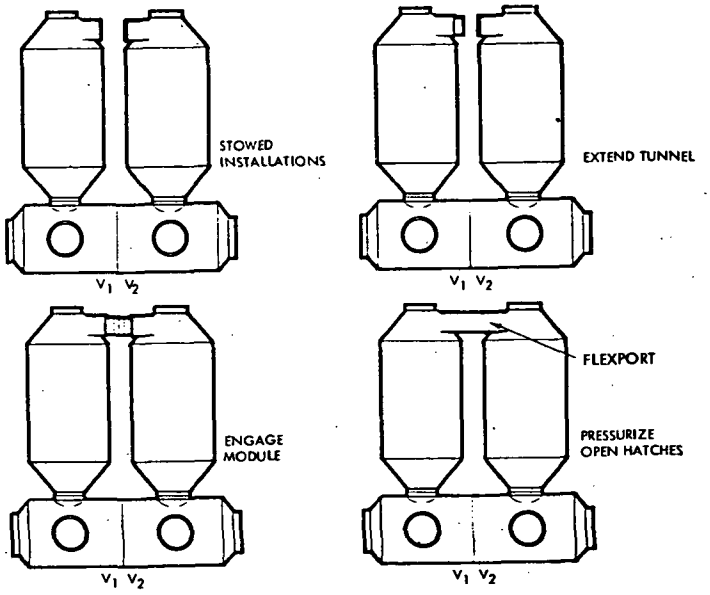

Figure 4.2-3. Flexports Between Modules

e) Minimum interchange of atmospheres between volumes in normal mode (to avoid cross-contamination, which, if carried to extremes, could preclude habitation of either pressure volume).

Table 4.2-2, below evaluates the safety advantages/disadvantages of normally keeping hatches open or closed against each functional requirement. Check marks imply advantages, and crosses disadvantages.

Table 4.2-2. Flexport Hatch Position Comparison

Functional Requirement	Open	Closed
a) Rapid opening	✓ Automatic.	X Crew action.
b) Shirtsleeve atmosphere	✓ Automatic.	X Requires valving.
c) Rapid shutting	X Increases the number of hatches to be closed including the core module hatch.	✓ Only the hatches that are used and the core module hatch need to be closed.
d) All hatches shut, & confirmed shut	X Increases the number of hatches to be closed including the core module hatch.	✓ Only the hatches that are used and the core module hatch need to be closed.
e) Minimum interchange of atmosphere	X Maximum.	✓ Minimum.

Bearing in mind that the flexports only have to be used in case of an emergency, and even then the normal means for exit will be into the core module; and also that no identified credible accident leads to an extremely time critical situation (i.e., requiring escape in seconds rather than minutes), primary importance is given to the factors (b), (d) and (e) in Table 4.2-2.

The recommendation is therefore made that flexport hatches normally be kept shut. To support this decision, the following additional requirements should be implemented.

a) The flexport hatches shall be designed for rapid, single action opening, and rapid, single action closing from both sides.

b) The flexport shall be designed so that its atmosphere is normally maintained at the same pressure as the station, and is suitable for rapid shirtsleeve passage of personnel. Following use in an emergency, the pressurization need not be maintained, but means for re-establishing a suitable pressure shall be provided.

c) Means shall be provided for shutting off any airflow across the hatches, e.g., for pressure equalization, from either side of each hatch. Remote shut-off of all hatches between pressure isolatable volumes shall be provided.

d) The open or closed status of each hatch shall be monitored at the control centers.

e) Operational procedures and/or design provisions shall be made for the rapid closure of flexport hatches so as to minimize or prevent cross-contamination of the atmosphere in the two pressure isolatable volumes.

Another decision, with Phase B impact, is whether the flexport hatches should open outwards (from the module) or inwards. Because of the immediately catastrophic consequences of an outward opening hatch accidentally opening (when a flexport is not connected to it), the hatches are required to open inwards, into the modules.

4.3 DUAL IVA/EVA ROUTES

There are a number of potential emergencies which will require intravehicular or extravehicular activity. The location, size, and number of IVA/EVA airlocks became an important safety considerations and have been found to exert some influence in the configuration of the modular space station. The most obvious use for an airlock is to allow entry into a depressurized or otherwise uninhabitable pressure volume. An IVA airlock must therefore be located at the interface of the two pressure volumes. Since an accident that caused the requirement for IVA also may result in damage to the airlock, a second means of obtaining access to the affected volume is required. It is acceptable for this backup means to involve some EVA activity.

Similarly, EVA access should be available by at least two independent routes, located or accessible from each of the two pressure volumes.

As configurational arrangements of the various modules have been developed, the location and arrangements for IVA and EVA airlocks have been integrated into the configuration. Figure 4.3-1 shows one of the potential modular space station configurations which has been considered. This contains an IVA/EVA airlock, shown shaded in the figure, between the two central core modules. This airlock could be used for either IVA or EVA from either of the two volumes. As a backup IVA mode for use if the central airlock could not be used, one of the crew quarter modules could be sealed off and depressurized, and the flexport used to obtain access to the other pressure volume. Backup EVA capability exists by using the same modules for performing EVA, and emergency EVA return also exists through one or more experiment airlocks, as well as through an airlock at the end of the power module, as shown in the figure. This arrangement exceeded the requirements for two independent ways of performing IVA and two for EVA.

The airlock must be sized to accommodate two men in a pressure garment assembly (PGA) with a backpack attached, because all IVA and EVA must be done using the buddy system. In this way one man can help the other in an emergency. This requirement resulted in a minimum size for each airlock of 30 square feet of area by 7 feet in height. Hatches must be capable of being opened from either side (after pressure equalization) and two PGA's must be located in each of the two pressure volumes.

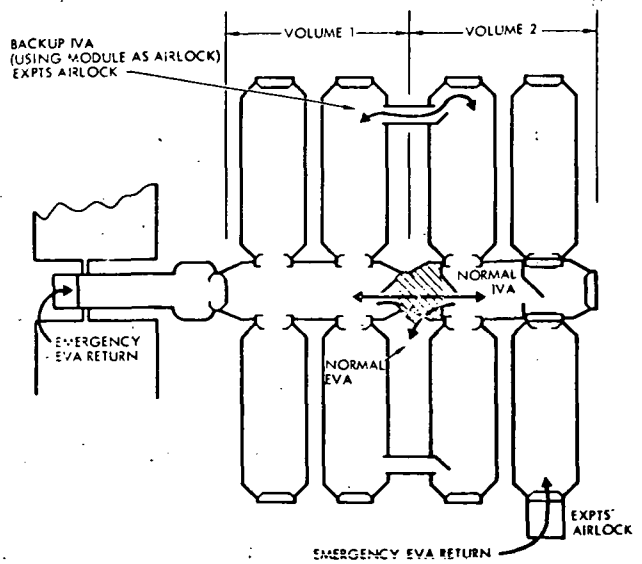

Figure 4.3-1. IVA/EVA Airlocks and Routes

One of the key considerations for IVA or EVA is the need to pre-breath pure oxygen to avoid the bends. This phenomonen could occur near 7 psi (from a 14.7 psi condition) and previously employed pressure suits operate at 3.5 to 5.0 psi with pure oxygen. The pre-breathing requirement could impose a severe restriction on the speed with which IVA or EVA can be performed, since it may take up to three hours to assure elimination of nitrogen from the blood stream. IVA and EVA could not, therefore, be a time-critical response to emergencies. Adequate supplies of pure oxygen would have to be available at each airlock location, and pre-breathing should be done before donning PGA's, however, in a 14.7 psi mixed atmosphere. These difficulties led to the consideration of a higher suit pressure where pre-breathing was not necessary. The advantages of a normal atmosphere soon outweighed the disadvantages and the higher suit pressure was selected as contributing to safety.

4.4 OPERATING MODES AND FAILURE/ACCIDENT TOLERANCE CRITERIA

The purpose of this section is to clarify the existing guidelines and criteria affecting the design of the MSS with respect to number of failures, and to describe certain operational modes related to these.

It became apparent that definition of the operational modes or plateaus of the space station following failures and/or credible accidents was required. In order to avoid semantics problems with the terminology, the various modes were described by the terms A, B. C. etc. The definitions of these modes are given in Table 4.4-1.

Table 4.4-1. Definition of Operational Modes

Operational Mode	Definition
A	All functions being performed within spec. No failures have occurred requiring maintenance.
B	All critical functions being performed within spec. Some failures have occurred requiring maintenance.
C	All critical functions are being performed, but some are out of spec. limits.
D	Crew can survive for 96 hours, but not until next scheduled Shuttle or One more failure can preclude crew survival for 96 hours.

In order to determine how much redundancy would be applied during the preliminary design of the MSS and to determine the level of this redundancy, Safety and Reliability criteria were established early in the Phase B Contract.

The criteria, Guidelines and Constraints, and definitions which are currently applicable to number of features from the NASA Guidelines and Constraints are listed below.

> Capability shall be provided for performing critical functions at a nominal level with any single component failures, or with any portion of a subsystem inactive for maintenance.
>
> Capability shall be provided for performing critical functions at a reduced level with any credible combination of two component failures, or with any credible combination of a portion of a subsystem inactive for maintenance and failure of a component in the remaining portion of the subsystem.

Specific applicability to the MSS resulted in the following:

> Capability shall be provided for performing critical functions at a nominal level.
>
> 1. With any single component failed, or
>
> 2. With any portion of the subsystem inactive for maintenance.

> Capability shall be provided for performing critical functions at a reduced level.
>
> 1. With any credible combination of two component failures, or
>
> 2. With any credible combination of a portion of the subsystem inactive for maintenance and a failure of a component in the remaining portion of the subsystem.

It is important to note that <u>component</u> failures are referred to in the criteria. These will generally correspond to IFRU failures, except where IFRU's have been designed so that no single component failure within the IFRU can cause failure of the critical function of the IFRU. In such a case, the IFRU failure should be counted as two component failures. In any event, the term "component" should not be confused with the definition of a level 7 item which is defined for purposes of costing in the MSS.

A <u>correct</u> application of the criteria would lead to two assemblies (each of which can still perform its function with any single component failed); to a design using one such assembly, with an alternate mode for performing the function and an emergency means for crew survival; or to many other possible combinations.

Since we are planning for the failure of components (i.e., we are expecting them to occur), an accident does not by definition, result simply from component failures. Some unexpected crew action, design, manufacturing or other defects, actions by the shuttle or other vehicles, or unexpected environments contribute to accidents. The station is required, by this section, to allow for crew survival following these. It should be noted that, generally speaking, accidents are situations, and are generally accepted as credible without having to justify exactly what combinations of events can lead to each accident. This is contrary to component failures, for which credible failure modes have to be identified.

The failure criteria apply to any component failures that impact the performance of critical functions and may be satisfied by providing redundancy within a subsystem or by alternate operating modes. The prime objective is to maintain critical functions to avoid loss of personnel during manned operations and continuation of the Space Station mission during buildup and manned operations. Tables 4.4-2 and 4.4-3 apply the general criteria to the MSS.

Table 4.4-2. Allowable Failure Criteria During Station Buildup - Premanning

Following:	Criteria Definition
1 component failure	The Station shall still be capable of being manned (shirtsleeve or IVA) for performance of maintenance and Station assembly tasks. This capability shall continue until arrival of the next scheduled Shuttle.
2 component failures	The Station shall still be capable of being manned (shirtsleeve or IVA) for at least 96 hours to accommodate an emergency Shuttle flight to perform maintenance.

Table 4.4-3. Allowable Failure Criteria During Manned Station Operations

Following:	Criteria Definition
1 component failure or any portion of a subsystem inactive for maintenance.	The Station shall still be capable of operating with all critical functions performed within specified values. This condition shall continue until maintenance can be performed.

Table 4.4-3. Allowable Failure Criteria During Manned Station Operations (Cont)

Following:	Criteria Definition
Any credible combination of 2 component failures. or 1 component failure with any portion of a subsystem inactive for maintenance. or Any credible accident (e.g., loss of any pressure isolatable volume).	The Station shall still be capable of operating with some critical functions performed at a reduced level, but not below the level necessary for crew survival. This condition shall continue until maintenance can be performed, but no more than 30 days or until arrival of the next scheduled Shuttle.
Any credible combination of 3 component failures. or Component failures and portions of a subsystem inactive for maintenance. or Any credible accident (e.g., loss of any pressure isolatable volume) and any single component failure.	The Station shall still be capable of crew survival for at least 96 hours to permit restoration of operations or rescue of the crew by emergency Shuttle.

An interpretation of the design criteria of Table 4.4-3, combined with the operational mode definitions of Table 4.4-1, lead to a set of operational criteria which determine permissible operational modes for the MSS following different numbers of failures (see Table 4.4-4). It is necessary to distinguish in this table between failures in critical functions and failures in non-critical functions. Suggested terminology for these operational modes or plateaus is included. Pictorially, the failure criteria for the manned

Table 4.4-4. Operational Criteria

Operational Mode	Allowable Number of Component Failures to Reach Operational Mode	
	Station Operation (Manned)	Build-Up (Unmanned)
A - Normal	0	0
B - Nominal	1	--
C - Degraded	2	1
D - Emergency	3	2

station operation are summarized in Figure 4.4-1. Requirements for redundant equipment were determined using the logic diagram of Figure 4.4-2.

A properly designed MSS would satisfy the failure criteria of Table 4.4-3 and the operational criteria of Table 4.4-4. Ideally, the space station design will meet these criteria. However, it was recognized that in practice, certain exceptions have to be made where it is either impossible or impractical to meet these criteria. These deviations were jointly identified, by the design groups in conjunction with Safety and Reliability personnel, and are published in the residual hazards and single point failure summaries.

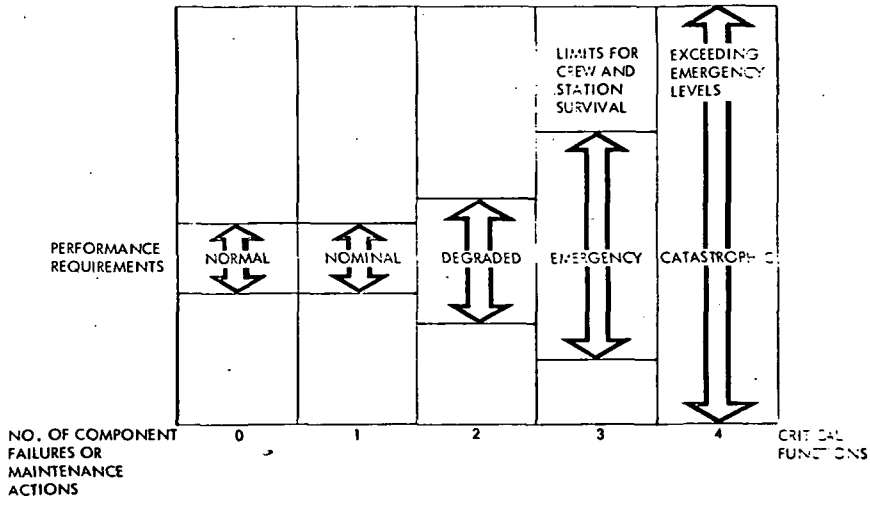

Figure 4.4-1. Performance Requirements as Related to Component Failures

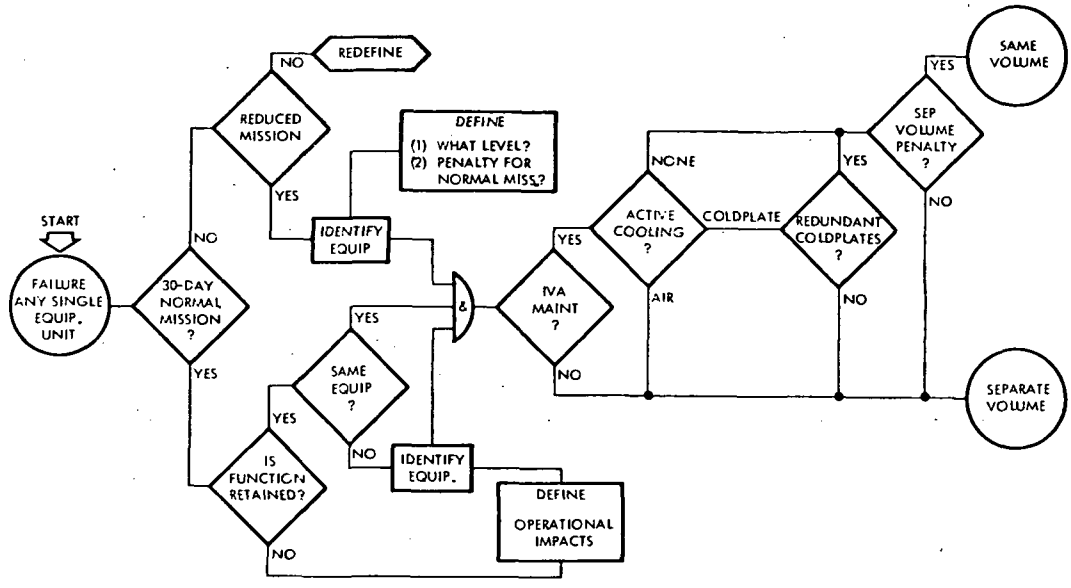

Figure 4.4-2. Logic Diagram for Determining Redundancy Requirements

4.5 PRESSURE VESSEL CRITERIA

An inevitable hazard on any space station configuration is the storage of various fluids in pressurized tanks for long periods. Since it was not possible to eliminate this hazard, steps were taken to minimize its potential effects and to make provisions in case of an accident.

Three main concerns arose with stored fluids. First, leakage of certain gases such as hydrogen, methane, or hydrazine could result in fire, explosion, or toxic effects; second, a large leakage rate inside a pressurized volume could cause overpressurization, leading to structural failure of the station; and third, a catastrophic rupture could cause damage to equipment, structural failure, and loss of life. A number of obvious precautions have been taken in the space station design. Every attempt has been made to locate hazardous and toxic fluid storage tanks and high-pressure tanks outside of pressurized and habitable volumes. Gases such as hydrazine have been avoided whenever possible because of their high toxicity. And, finally, for those tanks which must be placed inside the pressurized volume, every attempt was made to reduce the explosive potential of individual tanks and locate them so that an explosion of one tank would not propagate to adjacent ones.

The gases which are necessary on the station depend on the selection of atmospheric control, power, and reaction control systems. In all of the space station designs considered, large quantities of oxygen, hydrogen, and nitrogen have been required. Various means have been considered for preventing shrapnel from causing additional damage. These included use of chain link armor, blast shields, the use of blowout plugs oriented towards a safe direction, and the use of nonshattering tank material such as filament-wound fiberglass.

The explosive content of a stored gas, usually expressed in terms of TNT equivalent, depends primarily on the total energy content which can be released, and is approximately equal to the total enthalpy of the stored fluid. For a gas, this is proportional to the mass of the gas, the specific heat at constant pressure, and absolute temperature. The pressure at which a given mass of gas is stored relates to the TNT equivalent as shown in Figure 4.5-1. Since an explosion of a low-pressure tank could be as catastrophic as the explosion of the same mass of gas stored in a high-pressure tank, no attempt has been made to require storage tanks on board the station to be at low pressures for explosive reasons. However, damage assessment showed that an acceptable TNT equivalent for storage within the pressure volume could be approximately 0.025 pounds or 50 BTU's of energy (approximately the same as a hand grenade). While every attempt has been made to restrict on-board tanks to such a size, this became very difficult when the need for maintenance and replaceability of the tanks was considered.

A potential solution consisted of placing all of the high-pressure and hazardous gas storage tanks in a special module attached to the station externally. In this way, the hazardous gases were isolated away from the living and operating quarters. The outer hatch could be designed to accept

the blast from any credible explosion. The atmospheric pressure in this module would normally be kept low, but the module could be fully pressurized to allow crew access for maintenance, inspection, and resupply of individual tanks.

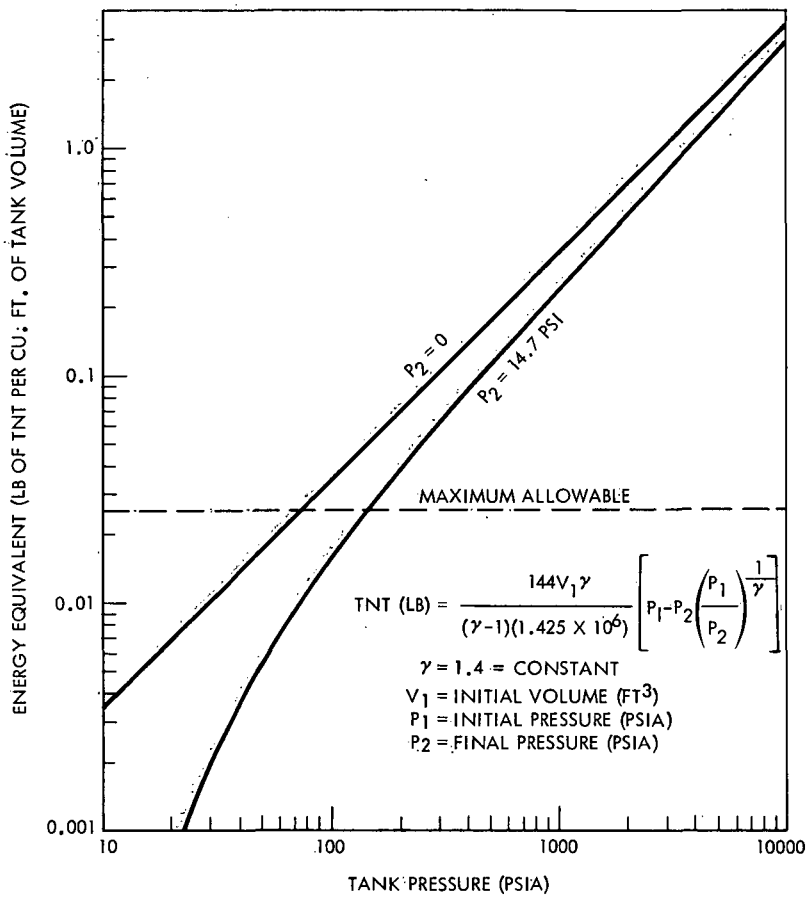

Figure 4.5-1. TNT Equivalent of Pressure Vessel

Much attention has been given to locating redundant tanks in widely different locations on the station, so that a catastrophic loss of one set of tanks would still allow continued operation of the station, at least until a rescue shuttle mission could remedy the situation. Fluids required for use in an emergency only, could be located in a single location, such as the special module discussed above, with provisions for supplying the fluids to either of the two pressurized volumes by appropriate plumbing.

The final design solution satisfied safety requirements by locating high energy tanks in the power boom and attached cargo module where crew exposure would be minimal. Since hydrogen and oxygen are generated by electrolysis during the solar exposure portion of the orbit and used in the fuel cells during the dark portion, it is necessary to store the gases in accumulators to a maximum pressure of 300 psi. Practically, these accumulators must

be located in the inhabited core and station modules together with the EPS, ECLSS and RCS subsystems. To minimize the hazardous effect of a bursting pressure vessel the energy content was limited by sizing. A conservative design safety factor of 4.0 was imposed to keep tank material strain well within the elastic range since the tanks operate as accumulators with constant pressure cycling over the ten-year life. The core module tanks will be designed to contain hydrogen and oxygen at 3000 psi (design factor 2.0) for RCS and fuel cell operation during build-up (unmanned) operations. After manning, these tanks will serve as accumulators with a maximum pressure of 300 psi, resulting in an operating safety margin of 20.

4.6 DOUBLE CONTAINMENT OF HAZARDOUS FLUIDS

The closed ecology cycle and limited volume make the MSS particularly susceptible to small leaks of hazardous fluids. Dilution of the module atmosphere with Freon could inhibit crew activities if a concentration of only 1000 ppm is reached. An increase in hydrogen gas concentration could reach explosive and fire limits well before cabin overpressure. On the other hand, release of oxygen would not immediately injury crew members, unless excessive leakage went undetected and increased the potential fire hazard. Also, an increase in nitrogen partial pressure would affect the module overpressure more than the crew.

In addition to indirect means of leak detection, such as pressure measurement, Freon and hydrogen tanks and lines are required to be enclosed in an outer shall for leakage containment. The intermediate volume will be maintained at pressures near cabin pressure and monitored for increase. Also, provision for venting this volume to space will be made as well as provision for dumping (to space) of the fluid remaining in the tank.

The electrolysis units are also a source of hydrogen and oxygen. Double-walled containment is required for this equipment in station modules.

4.7 HATCH PRESSURE EQUALIZATION

Large hatches required for crew egress with a PLSS or IVA suit develop large forces with small pressure differences. A typical airlock hatch opening in the core module has approximately 2600 square in. area. Handling of the hatch by a crew member could be hazardous if a residual pressure difference remained. Since force on the door is directly proportional to the pressure difference, 0.1 psi difference results in 260 lb force (Figure 4.7-1).

Three methods of hazard reduction have been used: 1) opening the door into the normally higher pressure volume, 2) providing a valved opening between the two compartments, and 3) measuring the pressure difference accurately. The first provision insures crewman safety by preventing hatch opening until the crewman strength is sufficient to swing the door against any remaining pressure difference. A second provision facilitates final pressure equalization. Electrically activated valving could provide an

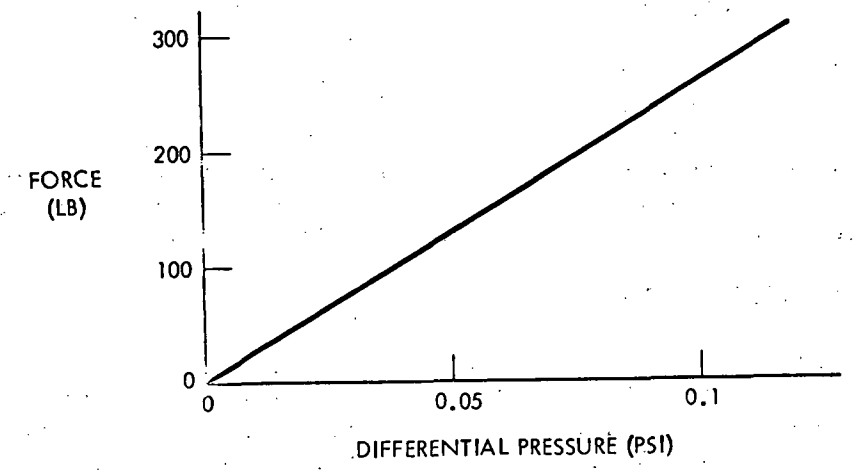

Figure 4.7-1. Force on Hatch Door Due to $\triangle$ P

opening with minimum crew effort. However, protection around the opening would have to be added to prevent high velocity gas flow and inadvertent coverage by the crew. The third method relies on sensitive measurements beyond the crew sensing capability. A combination of all three would provide the safest procedures. Additional methods, such as a mechanical hatch restraint that cracks the seal before full release, need to be investigated for optimum design feasibility.

4.8 METEROID PENETRATION

Penetration of the pressure wall by a meteroid will be a relatively rare event; however, the potential consequences of such an event must be considered.

The spacecraft structure is designed for no penetration by a meteroid defined by a certain probability of occurrence in a particular environment for the mission duration. Figure 4.8-1 shows the probability of no impact for a typical modular space station configuration during a 10-year mission. There is better than 0.999 probability of no impact by a meteroid larger than 1 gm mass and 15 mm (0.6 inch) diameter, and this size meteroid has been selected for defining the maximum credible meteroid penetration in the credible accidents. Such a meteroid would produce approximately 50 BTU's of energy inside the compartment it penetrated. This energy would be released in the form of heat, shock waves, and kinetic and thermal energy of finely divided molten high-speed shrapnel from spallation of the inner wall. This event was compared in magnitude to an explosion of a hand grenade and may be expected to injure personnel in the area, damage equipment, and start local fires. It also will result in a hole of approximately 2 inches in diameter in the pressure wall, approximately equal to the spacing between the meteroid bumper and the pressure wall.

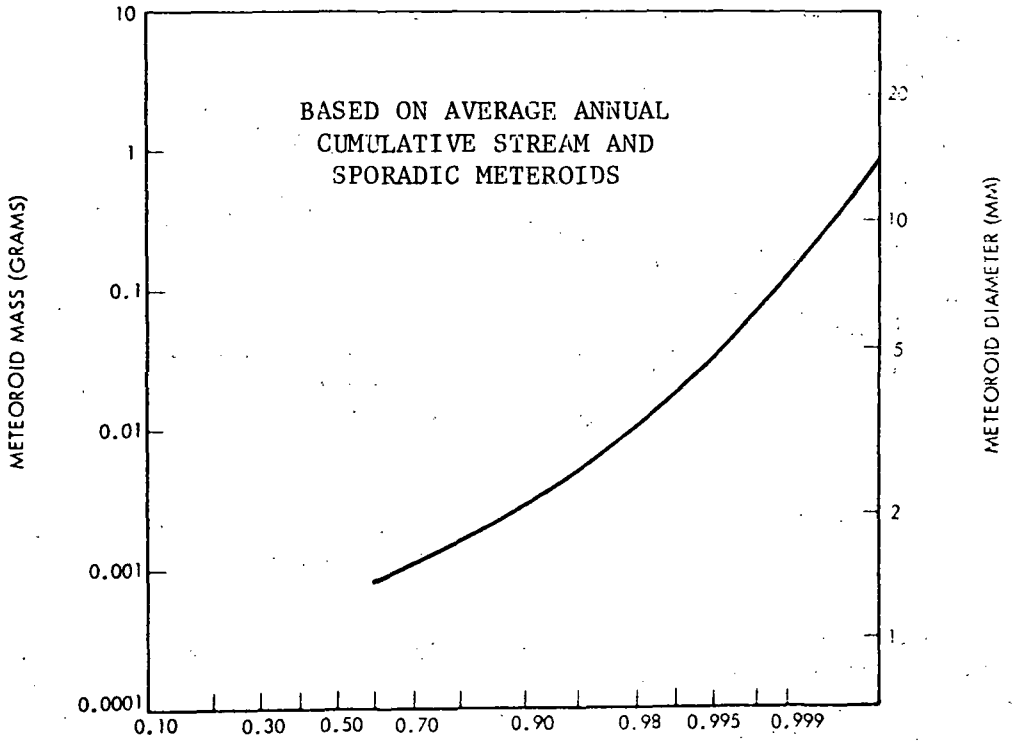

Figure 4.8-1. Probability of No Meteroid Impact

The depressurization effect from a penetration will depend on its size as well as the volume being depressurized. The pressure will decay exponentially with time and the crew will be able to function until a pressure of approximately 9.1 psi is reached. At this point, the partial pressure of oxygen will be 1.9 psi, and below this hypoxia may result in unacceptable levels of crew performance, with degraded visual performance. At a pressure of approximately 6.0 psi, loss of consciousness may result after a variable period, depending on individual susceptibility. Decompression sickness (bends) may occur if the pressure drops below 7.3 psi. Although the onset and course of this decompression sequence is unpredictable for any one individual, symptoms rarely appear during the first few minutes of exposure to the low pressure.

Figure 4.8-2 shows the decompression times to 9.1 psi for the maximum design case of a 2-inch penetration. If a single module were isolated, approximately five minutes of crew reaction time would be available for locating and making a temporary seal or for evacuating and sealing off the module. If several modules were open to each other, so that all of them share in the decompression, considerable more reaction time would be available. Operating the space station with the hatches open between modules, therefore, maximized the reaction time in the event of a leak, as well as allowing quicker access between the modules.

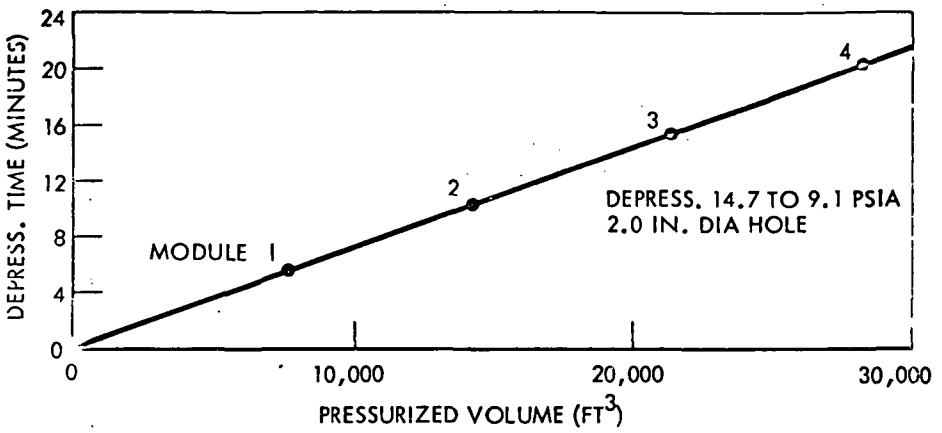

Figure 4.8-2. Effect of No. of Modules in Isolatable Volume on Depressurization Time

The 2-inch penetration represents a very severe case which would typically be encountered once in 10,000 years of space activity. As seen from Figure 4.8-1, meteroids with a more realistic probability of occurrence are considerably less massive and of smaller diameter. Although the size of penetration will not vary much, the energy released does decrease very rapidly with the size of the meteroid. Meteroids which are just beyond the structural capability of the primary structure will probably cause very small penetrations and the problem probably will be in detecting and locating them rather than in coping with damage.

4.9 DOCKING

Docking operations on both the Gemini and the Apollo programs have been conducted with a high degree of success. However, the docking problems encountered on the Apollo 14 flight highlight how failure to dock could have led to loss of mission. Inability of the shuttle to dock to the space station, could lead to loss of the station and of the on-board crew if EVA were not possible. Failure to undock from an attached sortie module or the station could also cause major problems to both vehicles, possibly leading to loss of one of the vehicles and to the need for a rescue mission.

The main safety concerns during docking arise from the possibility of exceeding the design criteria for the docking system. Contact at too high a velocity could result in damage to the docking mechanism or to the structure of either of the two vehicles.

The basic options available in the shuttle and station programs were to hard dock the shuttle to the station, free-fly and hard dock the payload (cargo module, experiments module or station modules) to the shuttle and station, or use manipulators on either shuttle or station for a soft docking

(berthing). All three methods had safety disadvantages which were factored into the trade. Hard docking of the shuttle to the station through an extended cargo module was very sensitive to errors in the docking parameters, particularly the approach velocity, because of the large masses of the two vehicles involved. The docking mechanism would have to be designed to absorb the relative energy at impact based on the maximum likely approach velocity as measured in simulated dockings with the available control systems.

The sensitivity of the docking maneuver to errors can be evaluated by considering the energy that must be absorbed by the docking system. This is, simply,

$$E = \frac{1}{2}\left[\frac{m_1\, m_2}{m_1 + m_2}\right] V^2$$

where m_1 and m_2 are the masses of the two vehicles and V is the relative approach velocity. The reduced mass term, $\frac{m_1\, m_2}{m_1 + m_2}$ is between 50 and 100 percent of the mass of the lighter vehicle. Therefore, relatively little energy has to be absorbed if one or the other of the two vehicles is relatively light (e.g., when the shuttle payload docks in a free-flying mode to station or shuttle). The energy is also relatively small if the contact velocity can be kept a low value.

One of the main advantages of manipulators was the low docking velocity that could be achieved, resulting in a lighter weight docking subsystem. Contact velocities of approximately 0.1 to 0.2 fps could be achieved with manipulators, compared to 0.5 to 1.0 fps for direct docking. An accidental collision would therefore be less severe with the manipulators. On the other hand the docking port designed for manipulator docking would be considerably more sensitive to approach velocity errors than the sturdier direct docking port.

This susceptibility is illustrated by the following example. The energy that has to be absorbed on docking is shown for the three docking methods considered in Table 4.9-1. Two accidents are considered in the table: in the first one the impact velocity is twice the design velocity and in the second it is a fixed increment of 0.5 fps higher than the design velocity. The excess energy that has to be absorbed (by the docking subsystem and the structure) is particularly large for the direct docking method and would be reflected in structural weight. The manipulator system is much more sensitive to a 0.5 fps error; where the total energy to be absorbed represents over 12 times the design case. The relative credibility of the two accidents then influences structural design and weight as well as control of the closing velocity.

Table 4.9-1. Energy Absorption for Design Conditions and Two Accident Situations

	Shuttle to Station Hard Dock	Module to Station or Shuttle Hard Dock	Shuttle to Station Manipulator Soft Dock
Design Contact Velocity (fps)	1.0	1.0	0.2
Energy Absorption (ft lb)			
Design Case	1,725 (E)	353 (E)	138 (E)
Accident: 2x Design Velocity	6,900 (4xE)	1,410 (4xE)	550 (4xE)
Accident: Design Velocity +0.5 fps	3,880 (2.25xE)	795 (2.25xE)	1,690 (12.25xE)
Weights: Shuttle = 250,000 lb Station = 200,000 lb Module = 25,000 lb			

The use of manipulators does make the docking operation safer with respect to impact damage. However, there are some potential failure modes associated with the manipulator which could result in loss of a station module, possibly the shuttle, and possibly the capability to continue the station program. Some of these situations are:

1. Failure of the shuttle manipulator to move.
2. Failure of the manipulator to stop moving.
3. Failure of the manipulator to grasp the station or a module.
4. Failure of any one docking port on the station where a redundant port is not available.
5. Failure of the shuttle to dock or undock.

The safety aspects of the docking options are not conclusive either for or against any of the options considered. Since adequate safety provisions can be made for any one of the three modes. The final safety selection can be made on the basis of which mode is least costly to make safe.

4.10 MANIPULATOR OPERATIONS

An overall analysis was made of the assembly functions to be performed by manipulators in order to determine potential single point failures at the program level.

Examination of the various operational concepts shows that the following potential failures are critical to building up the space station, i.e., the build-up cannot be completed if these failures occur.

1. Shuttle manipulator failure.
2. Failure of the manipulator "grab" mechanism on the shuttle.
3. Failure of the manipulator "grab" location on the station or module.
4. Failure of any one berthing port on the station where a redundant one is not available.
5. Failure to berth or unberth by the shuttle.
6. Failure to berth or unberth the shuttle docking adaptor to and from either the shuttle or the station.

Any of the above failures which cannot be circumvented by backup functions, becomes a single point failure to the program.

Analysis shows that there are potential means, some easily implemented and some difficult or undesirable, to prevent every one of the above six failures being single point program failures. The requirements for doing so are listed below; the number in the right hand column shows which of the six failures above drive the requirement. Where different requirements can be implemented, a generalized requirement is first stated, with the specific options indicated by the subscripts a, b, c. The asterisk ( )* indicates requirements which prevent single point failures leading to loss of a single module rather than the whole Space Station Program.

	Requirement	Failure Driving Reqmts.
1)*	Provide backup means for returning module to shuttle cargo in the event of shuttle manipulator failure.	1
2)*	Provide backup release on shuttle manipulator (required for shuttle safety, anyway).	1&2

	Requirement	Failure Driving Reqmts.
3)*	Provide multiple "grab" locations on each module.	3
4)	Provide multiple "grab" locations on the station at each stage of build-up.	3
5)	Provide continuation of build-up following damage to or malfunction of power module berthing port.	4
	5a)* Provide two berthing ports on power module	
or	5b)* Provide EVA capability to repair/replace/add-on berthing port on power module	
or	5c) Provide backup power module in program and design core module for survival until it can be brought up to orbit	
or	5d)* Design power module for return to Earth for repair, and design core module for survival until power module can br brought up again.	
6)	Provide a backup berthing port on the station at each stage of buildup, which allows shuttle berthing and a continuation of buildup.	4
7)	Provide continuation of buildup following damage to or malfunction of core module berthing port for berthing to power module.	4
	7a)* Provide two berthing ports (for power module) on core module	
or	7b)* Provide capability to maintain berthing port and mechanism (for power module) on core module in orbit	
or	7c) Provide backup core module in program and design power module to survive until it can be brought up to orbit	
or	7d)* Design power module to survive until core module can be returned to Earth, repaired, and returned to orbit.	
8)	Provide continuation of build-up following damage to or malfunction of berthing port on a common module.	4

Requirement	Failure Driving Reqmts.
8a)* Provide for survival of each stage of partially built-up station until module can be returned to Earth, repaired, and brought up to orbit again	
or 8b) Provide backup of each common module in program, and design for survival of each stage of partially built-up station until backup module can be brought up to orbit	
or 8c)* Design common modules for berthing at either end; i.e., two berthing ports per module	
or 8d)* Provide capability to maintain ports and mechanisms on common modules in orbit.	
9) Provide continuation of build-up following damage to or malfunction of berthing port on core module.	4
9a) Provide one more berthing port on each pressure isolatable volume of the core module than is required for normal build-up, capable of berthing any planned common module. Provide an emergency pressure-tight cover for damaged, leaking core module docking ports	
or 9b) Provide capability to maintain berthing ports and mechanisms on core module in orbit.	
10) Provide for survival of station until backup shuttle arrival in orbit.	5&6
11) Provide backup means for release of berthing ports.	5&6

In arriving at these requirements, it was assumed that a failure of a particular shuttle mission does not constitute program failure, and that the abandonment of any one station module in orbit is highly undesirable. If abandonment of one module is acceptable, the requirements identified with an asterisk are not needed.

A review of the above potential requirements to determine which are practical and desirable was made. It is recommended that the requirements underlined (e.g., 1) be included in the SRB.

Of these, four potentially difficult requirements to implement are:

- Provide backup means for returning module to shuttle cargo bay in the event of shuttle manipulator failure.

- Provide backup power module in program or design power module for return to Earth for repair; and design core module for survival until power module can be brought up to orbit again.

- Provide a backup berthing port on the station at each stage of buildup, which allows shuttle berthing and a continuation of buildup.

- Provide one more berthing port on each pressure isolatable volume of the core module than is required for normal buildup, capable of berthing any planned common module. Provide an emergency pressure-tight cover for damaged, leaking core module docking ports.

It may be programmatically acceptable to dispense with the first two requirements, thus accepting the following single point failures:

a) Inability of shuttle manipulator to berth a module to station, or return it to shuttle cargo bay. Rationale: This would lead, at worst, to loss of one station module.

b) Damage to or malfunction of power module berthing port, preventing berthing to core module. Rationale: Although this could lead to loss of the subsequent station program, it is a once-only operation with a high probability of success.

The last two requirements are considered a "must" however, since loss or damage of at least one berthing port is considered quite likely during the station program. It would therefore be unacceptable to have loss of any one berthing port constitute a single point failure.